VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

IMPLEMENTACE NÁSTROJE PRO ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI
IMPLEMENTATION OF A TOOL FOR CYBER SECURITY MANAGEMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Zuzana Strachová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Zuzana Strachová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Implementace nástroje pro řízení kybernetické bezpečnosti

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je implementovat vybraný automatizovaný nástroj, který ulehčí vedení organizace zajistit soulad s legislativním rámcem kybernetické bezpečnosti České republiky. Nástroj bude implementován v prostředí kritické informační infrastruktury. Výstupy práce by měly vést k zefektivnění řízení kybernetické bezpečnosti v organizaci.

Základní literární prameny:

ČSN EN ISO/IEC 27001 (369797). Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Druhé vydání. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. EAN 8590963958057.

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

KOLOUCH, J. a P. BAŠTA. CyberSecurity. Praha: CZ.NIC, 2019. ISBN ISBN 978-80-88168-34-8.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Svobodný přístup k informacím, Informatika, eGovernment. Ostrava: Sagit, 2020. 352 s. ÚZ, č. 1368. ISBN 978-80-7488-403-0.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D.
ředitel

doc. Ing. Vojtěch Bartoš, Ph.D.
děkan

Abstrakt

Diplomová práce je zaměřena na implementaci softwarového nástroje pro zvýšení efektivity řízení kybernetické bezpečnosti. Nástroj je implementován ve společnosti připravující se na zařazení do kritické informační infrastruktury. Na základě požadavků zadavatele je vybrán vhodný nástroj řízení kybernetické bezpečnosti. Následně navrhuji metodiku implementace nástroje, kterou vzápětí aplikuji. Výstupem práce je implementovaný nástroj, analýza rizik a ze zákona povinná bezpečnostní dokumentace.

Klíčová slova

analýza rizik, bezpečnostní audit, bezpečnost ICT, kritická infrastruktura, kritická informační infrastruktura, kybernetická bezpečnost, nástroj řízení kybernetické bezpečnosti

Abstract

The thesis is focused on the implementation of a software tool to increase the effectiveness of cyber security management. The tool is implemented in a company preparing to be classified as a part of critical information infrastructure. Based on the customer's requirements, a suitable cyber security management tool is selected. Subsequently, I propose a methodology for implementing the tool, which I immediately apply. The output of the work is an implemented tool, risk analysis and security documentation required by law.

Key words

risk analysis, security audit, ICT security, critical infrastructure, critical information infrastructure, cyber security, cyber security management tool

Bibliografická citace práce

STRACHOVÁ, Zuzana. *Implementace nástroje pro řízení kybernetické bezpečnosti* [online]. Brno, 2021 [cit. 2021-05-02]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133631. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 12. května 2021

.....

Bc. Zuzana Strachová

Poděkování

Mé poděkování patří Ing. Petru Sedlákovi za odborné vedení, přínosné rady a ochotu při konzultacích. Děkuji také společnosti za poskytnutí podkladů ke zpracování této diplomové práce, Ing. Petru Doleželovi za inspirativní zpětnou vazbu a všem dobrým lidem, kteří mi pomáhali.

V neposlední řadě chci poděkovat V. Havlovi a J. Werichovi, díky jejichž mimořádně obsažným životopisům, kterými jsem si podkládala notebook, mne při psaní tolik nebolela záda.

OBSAH

ÚVOD

Pierre Lévy, filozof a mediální vědec, specializující se mimo jiné na porozumění kulturním a kognitivním důsledkům digitálních technologií, ve svých dílech předestírá řadu inspirativních tezí. Některé z těchto tezí lze chápat jako nejobecnější východisko mé diplomové práce.

Dle autora pohyb směrem k virtuálnímu světu, prostřednictvím informačních technologií, začal ovlivňovat nejen oblast informací a komunikací, ale také naši fyzickou přítomnost, ekonomickou činnost, a dokonce i kolektivní rámec vnímavosti a způsobu realizace kognitivních výkonů. Virtualizační proces dokonce již stihl významně ovlivnit náš způsob existence prostřednictvím vzniku globálního virtuálního společenství a kybernetické kultury obecně. Tento nastíněný náhled byl autorem formulován v roce 1995, tedy z pohledu rychlého rozvoje informačních technologií velmi dávno. Autor uvádí proces digitální transformace do souvislosti s otázkami bezpečnosti, a to bezpečnosti obecné, bezpečnosti subjektivní (tzv. ontologické bezpečnosti) a bezpečnosti speciální tedy bezpečnosti ekonomické a technologické (1).

Lévyho představení kybernetického prostoru z filozofického nadhledu jako jakéhosi nového universa, nám pomáhá učinit si lepší představu, proč chránit toto virtuální „bohatství", respektive tyto virtuální entity, které v terminologii kybernetické bezpečnosti nazýváme aktiva. Lze také hovořit o ochraně virtuální komunity v širším smyslu.

Nezbytnost ochrany virtuálního prostoru ještě ostřeji nasvítila současná pandemická krizová situace, která výrazně zvýšila závislost společnosti na kybernetickém prostoru a informačních technologiích. Aktuálně jsme svědky mnoha úspěšných kybernetických útoků zejména na informační systémy státní správy, nemocnic a dalších subjektů. Útoky se odehrávají v době, kdy jsou tato zařízení v důsledku pandemie nejvytíženější a nejpotřebnější. Útočníci sází buď na ochotu oběti útoku rychle zaplatit výkupné, nebo se jedná o snahu prohlubovat nejistotu ve společnosti.

Vrcholná politická sféra, mimo jiné i díky množícím se bezpečnostním incidentům, začíná postupně přejímat narativ zásadní důležitosti kybernetické a informační bezpečnosti. Přirozenou prioritou se stává bezpečnost kritické informační infrastruktury, kde mohou mít případné škody vážný negativní dopad na chod státu a důležitých institucí. Škody způsobené útočníky neustále rostou a negativní dopady nejsou jen ekonomické,

ale i reputační, psychologické a politické. V oblasti tzv. kritické infrastruktury státu, kterou se zabývá má diplomová práce, pak mohou být důsledky podcenění kybernetické bezpečnosti dokonce až fatální.

Čím více činností se postupně přesouvá do kybernetického prostoru, tím automaticky narůstá význam kybernetické bezpečnosti. Narůstající komplexnost počítačových systémů a jejich datového obsahu představuje pro kybernetickou bezpečnost výzvu. Je třeba si uvědomit, že nedostatečná znalost vlastních aktiv nebo jejich faktického a právního kontextu vede ke snížení schopnosti je efektivně chránit. Kromě vlastního poznání strukturálních vlastností aktiv je nutné věnovat pozornost také identifikaci a definici jejich vlastníků. Kategorie vlastnictví v reálném světě je nám velmi dobře známá, a to včetně rizik plynoucích z nedostatečně vyjasněných vlastnických vztahů. Ve virtuálním světě je pojem vlastnictví mnohem obtížněji uchopitelný, i zde je však pojmem klíčovým. Exaktní popis obou klíčových předpokladů, tedy věcné struktury aktiv a určení jejich vlastnictví, tvoří základní komplexní předpoklad stanovení efektivní bezpečnostní strategie.

V mé diplomové práci se zabývám implementací nástroje pro řízení kybernetické bezpečnosti, který společnosti pomůže dosáhnout strukturovaného, přehledného a dostatečně exaktně definovaného pojetí řízení kybernetické bezpečnosti. Současně má nástroj přispět ke zvýšení povědomí o bezpečnosti a ke snížení bezpečnostních rizik. Objektivní potřeba této implementace vyplývá z možného zařazení analyzované společnosti do kritické informační infrastruktury, což automaticky vede ke zpřísnění požadavků na řízení kybernetické bezpečnosti. Implementovaný nástroj pomůže zajistit soulad s příslušnou legislativou.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

V diplomové práci je analyzována obchodní společnost (dále jen společnost), která spadá do prvků kritické infrastruktury v oblasti výroby elektřiny a poskytování podpůrných služeb. Vzhledem ke svému zaměření může být v budoucnu zařazena do kritické informační infrastruktury a podrobena auditu Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Z tohoto důvodu je společnost vystavena objektivní potřebě být dobře připravena plnit příslušné legislativní požadavky v oblasti kybernetické bezpečnosti. Vzhledem k důvěrné povaze některých shromážděných informací o společnosti, budou anonymizovány veškeré informace, které by mohly vést k její identifikaci.

1.1 Cíle práce

Hlavním cílem práce je implementovat vybraný softwarový nástroj, který umožní společnosti při jejím zařazení do kritické informační infrastruktury zajistit soulad s legislativním rámcem kybernetické bezpečnosti České republiky. K dosažení hlavního cíle práce je nutné nejdříve vymezit teoretický základ a provést analýzu současného stavu tohoto prvku kritické infrastruktury. Důležitým krokem analytické části je i výběr vhodného softwarového nástroje pro řízení kybernetické bezpečnosti a následná podrobnější analýza vybraného nástroje.

Po analýze bude následovat samotná implementace vybraného softwarového nástroje. Abych dospěla k úspěšné implementaci bezpečnostního nástroje, je potřeba stanovit a poté také dodržet metodiku jeho zavádění.

Dílčím cílem práce je zefektivnění řízení kybernetické bezpečnosti ve společnosti a tvorba povinné dokumentace v souladu se zákonem o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) ve znění pozdějších předpisů a vyhláškou o kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.) ve znění pozdějších předpisů. Tato snaha souvisí s potřebou připravit společnost na možný bezpečnostní audit NÚKIB.

V případě, že bude v průběhu realizace nalezen rozpor mezi funkcionalitou implementovaného nástroje a platnou legislativou, uvedu tento rozpor a navrhnu vylepšení. Důležitou částí práce bude časové a ekonomické zhodnocení, ze kterého

vyplyne finanční náročnost implementace spolu s posouzením návratnosti investice do bezpečnosti z hlediska investora.

1.2 Metody a postupy zpracování

Diplomová práce je rozdělena do čtyř hlavních částí, jedná se o část teoretickou, analytickou, návrhovou a ekonomické zhodnocení. V teoretické části vymezuji pojmy potřebné pro pochopení problematiky řízení kybernetické bezpečnosti, kritické informační infrastruktury, bezpečnostního auditu a upřesňuji další pojmy, které jsou relevantní pro praktickou (tj. analytickou a návrhovou) část. Hlavními informačními zdroji teoretické části jsou legislativní dokumenty, konkrétně vyhláška o kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.), zákon o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) ve znění pozdějších předpisů, normy vydané organizací ISO (*International Organization for Standardization*) řady ISO/IEC 27000 z oblasti bezpečnosti informací a pomocné materiály od NÚKIB.

Ve druhé části práce, která se zabývá analýzou současného stavu organizační a kybernetické bezpečnosti vybrané společnosti, vycházím z dat a informací poskytnutých společností, včetně interních dokumentů (tj. organizační, technické atd.) a výročních zpráv. Sběr doplňujících informací nezbytných pro implementaci softwarového nástroje je uskutečněn prostřednictvím řízených rozhovorů se zaměstnanci společnosti, konkrétně s manažerem kybernetické bezpečnosti a s jednotlivými garanty aktiv. Rozhovory jsou vedeny osobně nebo prostřednictvím elektronické pošty. Informace potřebné k analýze a výběru softwarového nástroje řízení kybernetické bezpečnosti jsou získány především z materiálů volně dostupných na internetu, popřípadě z produktových listů nástrojů zaslaných na vyžádání. K detailnější analýze konkrétního vybraného nástroje je využita SWOT analýza.

Metodika implementace v návrhové části vychází z doporučení vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, příslušných norem řady ISO/IEC 27000 a z manuálu získaného po zakoupení licence nástroje. Pro časovou analýzu je využita metoda síťové analýzy a Ganttův diagram. V ekonomickém zhodnocení realizace je aplikována metodika výpočtu návratnosti investic do zabezpečení: *Introduction to Return on Security Investment* (2) od bezpečnostní agentury ENISA.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V této části se zabývám objasněním pojmů a problematik, z nichž dále vycházím v analytické a návrhové části.

2.1 Vymezení základních pojmů

Bezpečnostní audit (*Security Audit*) je systematický, nezávislý proces zkoumání záznamu systému zpracování dat a testování adekvátnosti kontrol systému. Cílem auditu je zjistit do jaké míry se provozní postupy shodují s přijatou bezpečnostní politikou a zda jsou stanoveny odpovídající kontroly. Součástí auditu je i doporučení případných změn (v řízení, bezpečnostní politice a postupech) a návrh opatření. Audit může být prováděn externím (třetí strana) nebo interním auditorem (3).

Bezpečnostní opatření (*Security Control*) je prostředek řízení rizik, jehož smyslem je snížení míry rizika. Typicky existuje ve formě doporučení, postupů, pokynů, praktických úkonů nebo organizačních struktur, které mohou mít administrativní, technickou, řídící nebo právní povahu (4).

Bezpečnostní politika (*Security Policy*) je dokument, který vymezuje pravidla a zásady, které definují způsob zajištění ochrany aktiv v rámci organizace. Subjekty stanovené zákonem č. 181/2014 Sb., o kybernetické bezpečnosti mají povinnost vytvořit a schválit bezpečnostní politiky (5).

Data (*Data*) jsou vstupující a vystupující nehmotná aktiva informačního systému (IS), ukládaná, zpracovávaná a přenášená technickými prostředky (6, s. 15).

Dopad (*Impakt*) je výsledný negativní efekt realizované hrozby na organizaci, v jehož důsledku dojde ke kompromitaci důvěrnosti, vyzrazení, ztrátě integrity dat nebo zamezení dostupnosti informací, popřípadě informačního systému, včetně výsledného negativního vlivu na akceschopnost organizace, aktiva, jednotlivce, jiné organizace nebo vyšší celky, jako je například stát apod. (4).

Hrozba (*Threat*) je jakákoli okolnost nebo událost, která může nepříznivě ovlivnit systém, aktiva nebo celou organizaci a má potenciál poškodit poslání organizace, její funkci, reputaci, samotná aktiva nebo jednotlivce. Působení hrozby může způsobit

neoprávněný přístup, zničení systému, popřípadě odepření služby. Jako hrozba se označuje rovněž potenciál zdroje ohrožení úspěšně zneužít konkrétní chybu zabezpečení (4). Příkladem hrozby může být neúmyslná chyba zaměstnance, kybernetický útok, technická porucha zařízení nebo přírodní katastrofa (6, s. 57-58).

Informace (*Information*) je poznatek získaný z dat, který má smysl pro příjemce a/nebo pro toho, kdo jej vysílá (6, s. 15).

Norma (*Standard*) je dokument, vytvořený na základě konsensu a schválený všeobecně uznávaným orgánem nebo institucí, který stanoví zásady pro všeobecné a opakovatelné použití, pravidla, pokyny nebo charakteristiky pro činnosti nebo jejich výsledky, zaměřené na dosažení optimálního uspořádání v daném kontextu (4).

Riziko (*Risk*) je míra dopadu na provoz organizace, a to včetně jejího poslání, funkcí, pověsti, aktiv organizace nebo jednotlivců (4). Jedná se o potenciál hrozby využít zranitelnosti aktiva a poškodit tak organizaci (3).

2.2 Zranitelnost

Zranitelností (*Vulnerability*) je míněna potenciálně zneužitelná slabina systému. Zranitelnost informačního systému obvykle souvisí s nedostatečností bezpečnostních postupů, interních kontrol nebo přímo s nedostatky v návrhu, implementaci či nevhodném využití aktiva. Zranitelnost je taková slabina informačního systému, kterou může aktér hrozby (např. lidský útočník) zneužít k překročení definovaných hranic oprávnění a provést neoprávněnou akci v informačním systému. Úspěšné zneužití zranitelnosti vede k negativnímu dopadu na důvěrnost, integritu nebo dostupnost (triáda CIA). Aby mohl útočník zneužít zranitelnost, musí mít k dispozici alespoň jeden použitelný nástroj nebo postup (hrozba), který mu umožňuje využít zranitelnost (4).

V kybernetické bezpečnosti lze zranitelnosti rozdělit na zranitelnosti známé (opravené, neopravené) a zranitelnosti neznámé (skryté, neobjevené). Zranitelnost, na kterou není vydána záplata je označována jako tzv. zranitelnost nultého dne (*Zero-day Vulnerability*). Tento pojem označuje takovou zneužitelnou zranitelnost, která není známá straně, která je odpovědná za opravu nebo odstranění chyby. Za této situace má útočník znalý dané zneužitelné zranitelnosti značnou výhodu (7, s. 479).

2.3 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací, také známý pod anglickou zkratkou ISMS *(Information Security Management System)*, je soubor bezpečnostních politik, postupů, pravidel, směrnic, příslušných zdrojů a činností organizace zajišťující ochranu informačních aktiv. ISMS je založen na systematickém přístupu (včetně dokumentace) k ustavení, implementaci, provozu, monitorování, přezkoumání, udržování a konstantnímu zlepšování bezpečnosti informací v organizaci. Cílem ISMS je efektivně řídit rizika a zajistit kontinuitu činností organizace (8). ISMS vymezují normy ISO/IEC řady 27000 i vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (VKB).

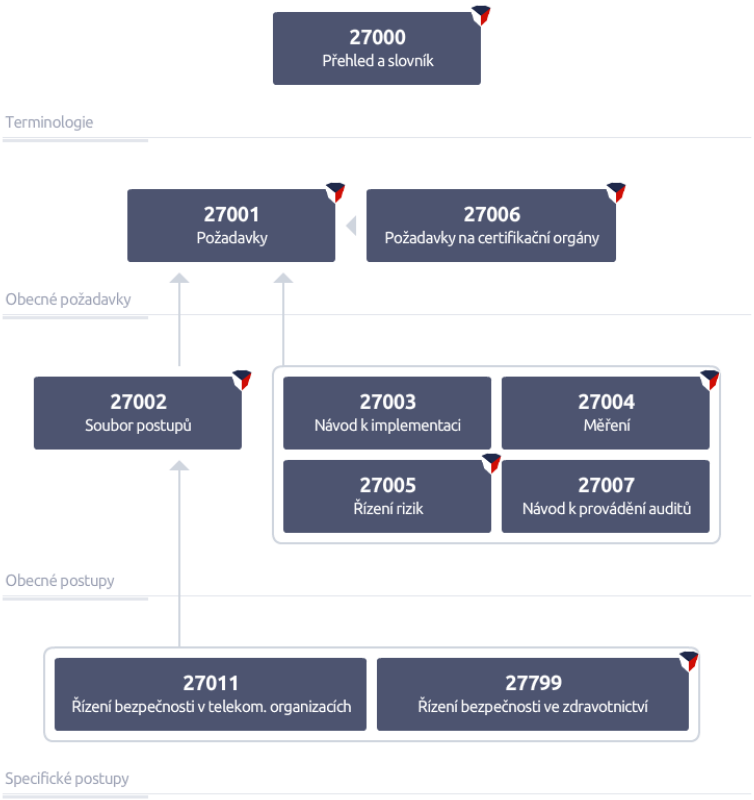
Dle VKB (§ 3) je postup v rámci systému řízení bezpečnosti informací následující:

- stanovení rozsahu ISMS (dotčené organizační části a aktiva),
- stanovení cíle ISMS,
- zavedení vhodných a přiměřených bezpečnostních opatření,
- řízení rizik,
- vytvoření a schválení bezpečnostní politiky ISMS (součásti – hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací) a zavedení adekvátních opatření v dalších oblastech ISMS,
- provedení auditu kybernetické bezpečnosti, informačního a komunikačního systému,
- zajištění pravidelné kontroly účinnosti ISMS (hodnocení stavu systému řízení bezpečnosti informací, revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů bezpečnostních incidentů),
- průběžné řízení významných změn, udržování aktuálnosti ISMS a příslušných dokumentů, řízení provozu a zdrojů ISMS (5).

2.3.1 Normy řady 27000

Řada norem ISMS (ISO/IEC 27000) jsou technické normy specifikující požadavky ISMS (ISO/IEC 27001) a požadavky certifikačních orgánů (ISO/IEC 27006). Normy rovněž poskytují návody na implementaci, následné udržování a zlepšování ISMS (včetně specifikace dle odvětví). Normy jsou vydané Mezinárodní organizací pro standardizaci označovanou jako ISO (*International Organization for Standardization*) (8).

Na obrázku 1 je zobrazen přehled základních norem řady ISMS s vyjádřenými vzájemnými vztahy a popisem jejich zaměření.



Obrázek 1: Vybrané normy řady ISO/IEC 27000 (Zdroj: (9))

2.4 Kybernetický prostor

Lévy definuje kybernetický prostor (*Cyberspace*) jako „*komunikační prostor otevřený vzájemným světovým propojením počítačů a počítačových pamětí*" (10, s. 83).

NIST (*National Institute of Standards and Technology*) definuje kybernetický prostor jako vzájemně závislou síť tvořenou infrastrukturou informačních systémů včetně internetu a sítí elektronických komunikací: Jedná se o digitální prostor, kde dochází k interakci lidí, softwaru a služeb pomocí technologických zařízení tvořících propojenou síť (4).

Kybernetický prostor umožňuje vznik, výměnu a zpracování informací (3). V roce 2016 byl kybernetický prostor zařazen mezi operační domény NATO (11).

2.5 Kybernetická bezpečnost

Kybernetická bezpečnost zajišťuje ochranu kybernetického prostoru pomocí právních, technických, organizačních, nebo vzdělávacích prostředků (3).

NIST definuje kybernetickou bezpečnost jako ochranu, obnovu a prevenci před poškozením informačních a komunikačních systémů včetně informací v nich obsažených tak, aby byla zajištěna jejich dostupnost (*Availability*), integrita (*Integrity*), důvěrnost (*Confidentiality*), autentičnost (*Authentication*) a nepopiratelnost (*Nonrepudiation*) (4).

Pro porovnání informační bezpečnost se zabývá ochranou informací po celý jejich životní cyklus. Toto širší pojetí informační bezpečnosti abstrahuje od typu nosiče informace. Z hlediska informační bezpečnosti tedy může být informačním médiem stejně tak například papír nebo fyzická fotografie jako elektronické médium apod. (7, s. 46).

Na obrázku 2 je znázorněn životní cyklus kybernetické bezpečnosti spočívající v neustále se opakujícím procesu analýzy rizik, definování příslušných opatření, zavedení opatření pro eliminaci rizik, správě celého procesu a interního i externího auditu.

Obrázek 2: životní cyklus kybernetické bezpečnosti (Zdroj: (12))

2.6 Triáda CIA

Nejpoužívanější triádou informační a kybernetické bezpečnosti je triáda CIA.

Jednotlivá písmena triády značí následující atributy:

- C – Confidentiality (*důvěrnost*),
- I – Integrity (*integrita*),
- A – Availability (*dostupnost*) (13).

Atributy CIA představují základní principy informační (kybernetické) bezpečnosti. Použití triády CIA pomáhá společnosti při tvorbě bezpečnostních politik (13).

Důvěrnost (*Confidentiality*) je vlastnost zajišťující dostupnost informace pouze pro oprávněné (autorizované) entity, jednotlivce, procesy (3). Důvěrnost může být zajištěna například šifrováním, dvoufázovým ověřením, bezpečnostními tokeny atd. Dalším vhodným opatřením proti narušení důvěrnosti je školení uživatelů v oblasti osvědčených postupů tvorby hesel a nástrah sociálního inženýrství (13).

Integrita (*Integrity*) je vlastnost, která zajišťuje úplnost a přesnost informací (3). Mezi opatření pro zajištění integrity patří řízení přístupu a verzování, data mohou zahrnovat kontrolní součty nebo elektronické podpisy. K obnovení poškozených dat se využívá zálohování (13).

Dostupnost (*Availability*) je vlastnost, která umožňuje na žádost (tj. v okamžiku této žádosti) oprávněné entitě přístup k informacím a jejich použitelnost (3). Dostupnost se zajišťuje preventivními opatřeními jako je redundance, důsledná údržba hardwaru, udržování aktuálnosti systému, vyhotovení tzv. Disaster recovery plánu, geograficky oddělené umístění záložních kopií atd. (13).

Kybernetická bezpečnost se zabývá ochranou informací a dat, ale i počítačových systémů a kybernetického prostoru, v němž jsou data přenášena. Triáda CIA by se měla aplikovat na samotné informace i na další prvky kybernetické bezpečnosti jako jsou zmíněná data, počítačové systémy atp. (7, s. 48).

2.7 Kybernetická kriminalita

Kolouch ve svém souhrnném díle CyberCrime (14) definuje kybernetickou kriminalitu (respektive počítačovou kriminalitu) více různými způsoby. Za nejobecnější zde obsaženou definici kybernetické kriminality lze považovat následující charakteristiku.

Kybernetická kriminalita je kriminalita, při které *„jsou prostředky informačních a komunikačních technologií použity jako nástroj pro spáchání trestného činu”* nebo *„jsou cílem útoku pachatele”.* Útok je trestným činem, pokud *„jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí (tedy v kyberprostoru).*” (14, s. 36)

Současně autor konstatuje existující značné neshody ve stávajících definicích i chápání kybernetické kriminality jako takové. Jedná se o logický důsledek skutečnosti, že se tento obor v současnosti teprve etabluje (14).

2.8 Legislativa kybernetické bezpečnosti

Základní právní předpisy upravující kybernetickou bezpečnost na území České republiky jsou popsány v následujících podkapitolách.

2.8.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů, dále jen ZKB, vymezuje kybernetickou bezpečnost a kybernetický prostor, povinné subjekty, základní úroveň bezpečnostních opatření, upravuje práva a povinnosti subjektů v rámci kybernetického prostoru, upravuje působnost dohledových pracovišť v oblasti kybernetické bezpečnosti, stanovuje povinnost hlášení bezpečnostních incidentů, vymezuje vládní a národní CERT, definuje případné sankce za nedodržení povinností a nápravná opatření (15).

Zákon vychází z příslušných právních předpisů Evropské unie (EU) a byl několikrát novelizován (poslední novelizace proběhla zákonem č. 12/2020 Sb.) (16).

Základními povinnými subjekty ZKB jsou správci a provozovatelé informačního nebo komunikačního systému kritické informační infrastruktury, správci a provozovatelé významných informačních systémů, správci a provozovatelé informačního systému základní služby, poskytovatelé digitálních služeb, poskytovatelé služby elektronických komunikací a subjekty zajišťující síť elektronických komunikací (15).

Dohled nad plněním povinností stanovených ZKB vykonává Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) (15).

2.8.2 Směrnice NIS

Směrnice NIS je *směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*. Cílem směrnice je zajištění souladu právních úprav států

EU v oblasti bezpečnosti sítí a informačních systémů a zavedení jednotného standardu úrovně kybernetické bezpečnosti (16).

Směrnice NIS rozšířila povinné subjekty o provozovatele základní služby a poskytovatele digitálních služeb (internetové vyhledávače, cloud computing a online tržiště). Toto rozšíření je již zapracováno v novele ZKB z roku 2017 a ve VKB (16).

2.8.3 Vyhláška kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) ve znění pozdějších předpisů, dále jen VKB, zapracovává směrnici NIS. Vyhláška je platná pro subjekty definované ZKB (5).

VKB upravuje obsah a strukturu povinné bezpečnostní dokumentace, definuje bezpečnostní opatření, stanovuje typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, ukládá způsob hlášení kybernetických bezpečnostních incidentů a upřesňuje náležitosti oznámení o provedení reaktivních opatření a jejich výsledcích. Nově se oproti vyhlášce č. 316/2014 Sb. zabývá způsobem likvidace dat, provozních údajů, informací včetně jejich kopií (5).

Součástí přílohy VKB jsou stupnice hodnocení (důvěrnost, integrita, dostupnost), hodnocení rizik, zranitelnost a hrozby a vzor oznámení kontaktních údajů (5).

2.9 Kybernetická bezpečnostní událost a incident

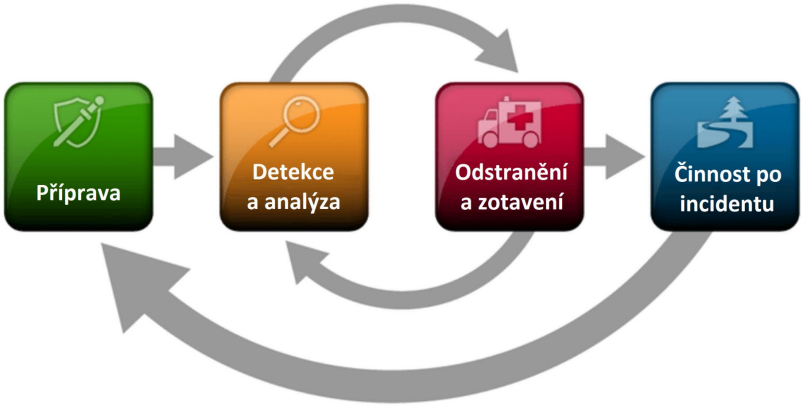
Při definování následujících pojmů vycházím z platného ZKB.

Kybernetická bezpečnostní událost (*Cyber Security Event*) nastává po pokusu o realizaci hrozby nebo po realizaci hrozby a může *„způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací"* (15).

Kybernetický bezpečnostní incident (*Cyber Security Incident*) vzniká v důsledku bezpečnostních událostí. Jedná se o „*narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací"* (15).

2.9.1 Životní cyklus reakce na incident

Speciální publikace NIST *Computer Security Incident Handling Guide* uvádí čtyři fáze reakce na incident (17). Tyto fáze jsou vidět na obrázku 3.



Obrázek 3: Fáze životního cyklu reakce na incident podle NIST (Zdroj: Vlastní zpracování dle (17))

Počáteční *přípravná fáze* spočívá v založení a následném školení týmu pro reakci na incidenty a v zajištění potřebných zdrojů. Příprava zahrnuje vyhodnocení analýzy rizik na jejímž základě se následně implementují opatření potřebná k omezení počtu incidentů. I po implementaci opatření však přetrvávají zbytková rizika. V případě, že nastane incident narušující bezpečnost a je *detekován* (varování pro organizaci) následuje *analýza* incidentu. Následně se organizace snaží dopady incidentu *odstranit* a *zotavit* se z něj. V této fázi často dochází k návratu k předešlé fázi (např. za účelem zjištění, zda jsou malwarem infikovány další části systému). Po adekvátním vyřešení incidentu následují *činnosti po incidentu*, které zahrnují vydání reportu s popisem příčiny, nákladů incidentu a kroků, které organizace podnikne, aby zabránila budoucím incidentům stejného typu (17).

2.10 NÚKIB

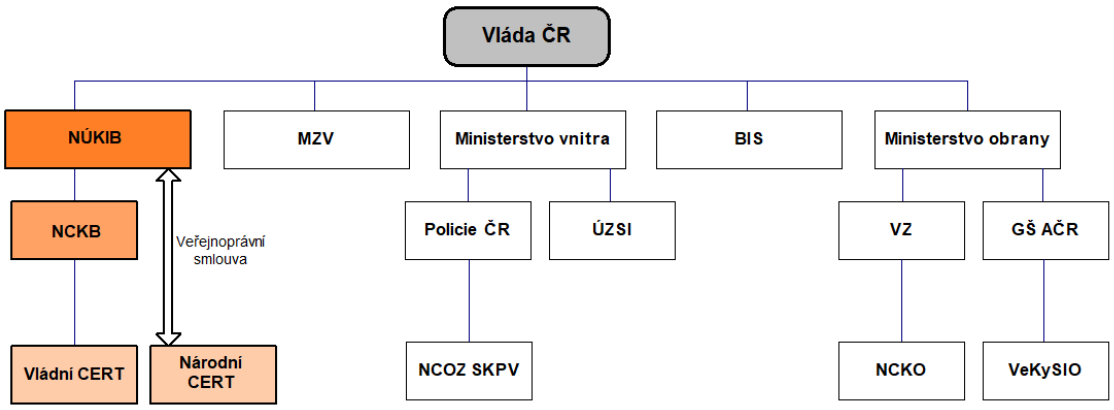
Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je správní úřad ČR v oblasti kybernetické bezpečnosti, kryptografické ochrany a ochrany utajovaných informací, které jsou součástí informačních a komunikačních systémů. Tento úřad byl

ustaven na základě novely zákona o kybernetické bezpečnosti (zákon č. 205/2017 Sb.) (18).

Mezi kompetence NÚKIB patří také tvorba bezpečnostních standardů a příprava legislativy pro kybernetickou bezpečnost, pořádání kybernetických cvičení, výzkum a vývoj, určování národní strategie kybernetické bezpečnosti a spolupráce s bezpečnostními týmy CERT a CSIRT v ČR i celosvětově, přičemž tzv. vládní CERT České republiky (GovCERT.CZ) spadá přímo pod NÚKIB (18).

Výkonnou složkou NÚKIB je Národní centrum kybernetické bezpečnosti (NCKB) (19).

Obrázek 4 znázorňuje schéma ukotvení NÚKIB, NCKB a týmů CERT (viz kapitola 2.11) ve strukturách vlády ČR.



Obrázek 4: Schéma ukotvení NÚKIB ve strukturách ČR (Zdroj: Vlastní zpracování dle (11, s. 8))

2.11 CERT, CSIRT, SOC

CERT (*Computer Emergency Response Team*) *Tým pro reakci na nouzové situace*

Na základě ZKB byly na území České republiky zřízeny dva týmy typu CERT, a to vládní a národní. Dle ZKB mají týmy CERT plnit také roli týmu CSIRT (15).

Vládní CERT je provozován NCKB pod názvem GovCERT.CZ a má za úkol řešit bezpečnostní incidenty především s veřejnou správou, provozovateli kritické informační infrastruktury, provozovateli významných informačních systému, systémů základní služby a digitální služby (15). Úkolem vládního CERT je také vydávat varování před kybernetickými hrozbami, doporučovat opatření (reaktivní a preventivní), poskytovat metodickou podporu, osvětovou a vzdělávací činnost, spolupracovat s národním CERT týmem a přijímat jeho hlášení (19).

Národní CERT je nevládní sdružení kvalifikovaných odborníků, provozováno pod názvem CSIRT.CZ. Zabývá se řešením bezpečnostních incidentů, které neřeší vládní CERT. Zaměřuje se zejména na osoby soukromého práva. Role národního CERT týmu byla na základě veřejnoprávní smlouvy svěřena sdružení CZ.NIC (20). Národní CERT, který spadá pod CSIRT.CZ zajišťuje dle ZKB proaktivní služby, včetně sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti, osvětové a školící činnosti. Současně plní roli koordinátora národního týmu CSIRT (*Cyber Security Response Team*) a spolupracuje v této oblasti s Evropskou unií (EU) (15).

Na území ČR spolupracuje konkrétně se subjekty poskytujícími internetové připojení, poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem a úřady státní správy. V celosvětovém měřítku pak s rozsáhlou komunitou CERT/CSIRT týmů (20).

CSIRT (*Computer Security Incident Response Team*) *Tým pro reakci na bezpečnostní incidenty*

CSIRT jsou skupiny vznikající přímo v organizacích. CSIRT týmy se zaměřují na všechny etapy životního cyklu reakce na incident (viz kapitola 2.9.1) v rámci organizace i mimo ni. Mají-li kompetence, řeší incidenty přímo, popřípadě řešení incidentu koordinují. CSIRT týmy jsou propojené se světovou bezpečnostní infrastrukturou a mezi jejich povinnosti patří sdílení informací o incidentech a hrozbách (21). V ČR spadá pod CSIRT.CZ i národní CSIRT (20).

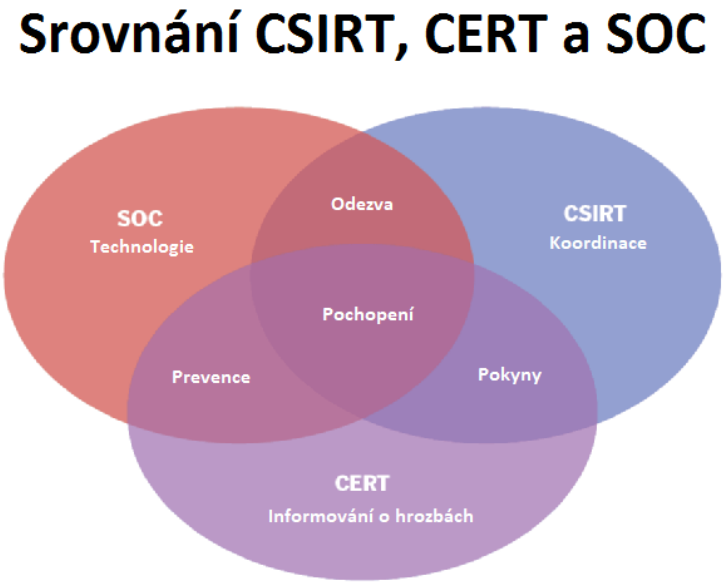
Proces hlášení kybernetického incidentu probíhá na:

- Vládní CERT pro systémy spadající pod ZKB.
- Národní CERT pro systémy, které nespadají pod ZKB (15).

SOC (*Security Operations Center*) *Bezpečností operační centrum*

SOC je tým odborníků v libovolné organizaci zaměřený na průběžné monitorování a analýzu kybernetické bezpečnosti. Cílem SOC týmu je detekovat a analyzovat hrozby a odpovídajícím způsobem na ně reagovat pomocí nejvhodnější kombinace technických, organizačních a provozních opatření (22).

Týmy CSIRT, CERT a SOC hrají klíčovou roli pro účinné řízení incidentů a kybernetickou ochranu. Jejich vztah je definován a znázorněn na obrázku 5 (22).



Obrázek 5: Vazby CSIRT, CERT a SOC (Zdroj: Vlastní zpracování dle (22))

Na obrázku 5 jsou v průnicích CSIRT, CERT a SOC zobrazeny potřebné procesy – odezvy (*Response*), prevence (*Prevention*), pokyny (*Guidelines*) a pochopení (*Understanding*). Týmy CSIRT a CERT se zaměřují konkrétně na reakci a incidenty. Jejich úkolem je poskytovat podporu pro orgány státu, organizace i jednotlivé občany. Působnost SOC je komplexnější a nejedná se pouze o reakci na incidenty. Jde o centralizaci řízení bezpečnostních událostí a incidentů s cílem minimalizovat reakční doby na incident a škody způsobené incidenty. Působnost SOC je rozšířená i o další oblasti kybernetické bezpečnosti (22).

2.12 Aktivum

Aktivum (*Asset*) v daném kontextu chápeme jako něco, co je potřeba chránit, protože má pro organizaci (nebo jednotlivce) určitou hodnotu. U každého aktiva by měl být definován vlastník aktiva nebo také garant aktiva (viz kapitola 2.13.3) (23).

2.12.1 Primární aktivum

Primárním aktivem se dle VKB rozumí *„informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém“* (5).

Dle ISO/IEC 27005:2013 se jedná o obchodní procesy, činnosti a informace, zejména hlavní procesy organizace a informace o těchto procesech (činnostech) v rámci stanoveného rozsahu. Primární aktiva identifikuje příslušná skupina zástupců procesů, jako jsou vedoucí pracovníci, odborníci v oblasti informačního systému nebo uživatelé (23).

2.12.2 Podpůrné aktivum

Podpůrným aktivem se dle VKB rozumí *„technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému“* (14).

Následující rozdělení podpůrných aktiv vychází z normy ČSN ISO/IEC 27005:2013.

Základní rozdělení spolu s výčtem příkladů:

- **Hardware –** zařízení pro zpracování dat, pevná zařízení, přenosná zařízení, periferní zařízení pro zadání, prezentaci či přenos dat, kamerové systémy, elektronické nosiče dat, neelektronické nosiče dat.
- **Software** – operační systém (OS) včetně všech programů, souborů systémových služeb a prvků, software (SW) pro služby, údržbu nebo správu, SW balíky a standardní SW, podnikové aplikace.
- **Sítě** – veškerá telekomunikační zařízení využívaná k propojení počítačů a prvků informačního systému, komunikační a telekomunikační média a zařízení zprostředkující nebo transportní zařízení, komunikační rozhraní procesních jednotek.
- **Pracovníci** (zohledněno u aktiv při hodnocení hrozeb/rizik) – pracovníci, zabývající se provozem a údržbou informačních a komunikačních systémů, vedení, vlastníci primárních aktiv, uživatelé, kteří manipulují s citlivými prvky mající zvláštní odpovědnost, vývojáři aplikací.
- **Lokalita** (zohledněno u aktiv při hodnocení hrozeb/rizik) – lokality v rozsahu identifikovaných aktiv a fyzické prostředky nutné pro provoz těchto aktiv.

- **Fyzická místa –** vnější prostředí, na které nemohou být uplatněny bezpečnostní prostředky společnosti, areál (prostory) společnosti, zóny tvořené fyzickou ochrannou hranicí rozdělující prostory uvnitř areálu společnosti, chránící informační a komunikační infrastrukturu organizace, služby nezbytné pro provoz organizace, telekomunikační služby a zařízení, poskytované operátorem, služby a prostředky pro zajištění elektrické energie pro zařízení a periferie IT, služby.
- **Organizace** (zohledněno u aktiv při hodnocení hrozeb/rizik) – struktura pracovníků, řídících pracovníků/ pracovníků zajišťujících chod klíčových procesů a činností společnosti, celková organizační struktura, projektové řízení, vytvořené pro řízení konkrétních projektů či služeb, (sub)dodavatelé poskytující služby nebo zdroje na základě smlouvy (23).

2.13 Bezpečnostní role

V následujících podkapitolách jsou vymezeny bezpečnostní role dle VKB.

2.13.1 Povinná osoba

Povinná osoba je *„orgán nebo osoba, která je povinna zavést bezpečnostní opatření podle zákona (ZKB)“* (5).

V § 3 písm. c) ZKB je jako povinná osoba v oblasti kybernetické bezpečnosti definován *„správce a provozovatel informačního systému kritické informační infrastruktury“* což je relevantní pro účely této diplomové práce (15). Povinná osoba určuje složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, garanta aktiva, auditora kybernetické bezpečnosti. Dále zajišťuje zastupitelnost manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti (5).

Doporučené požadavky na bezpečnostní role obsahuje Příloha č. 6 k vyhlášce č. 82/2018 Sb. (5).

2.13.2 Výbor pro řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti *„je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení*

bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností“ (5).

Mezi členy musí být zařazen alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. Výbor je odpovědný za tvorbu rámce kybernetické bezpečnosti, definování strategických cílů a směřování rozvoje v oblasti kybernetické bezpečnosti, definuje role a jejich odpovědnosti, definuje požadavky na podávání zpráv a provádí kontrolu systému řízení bezpečnosti informací a v neposlední řadě kontroluje aktuální stav kybernetické bezpečnosti a naplnění plánovaných cílů (5).

2.13.3 Vlastník (garant) aktiva

ČSN ISO/IEC 27002 definuje vlastníka aktiva jako jednotlivce (popřípadě entitu), který je odpovědný za správu, řízení a kontrolu aktiva po celý životní cyklus. Vlastník je určen a svou roli potvrzuje, nemusí mít však vlastnické právo (rozuměj věcné právo v právním smyslu) k danému aktivu (24).

VKB zavádí pojem garant aktiva, kterého definuje jako *„bezpečnostní roli odpovědnou za zajištění rozvoje, použití a bezpečnost aktiva“* (5).

Role by měla být přidělena člověku s dobrou znalostí aktiva, měl by se orientovat v interních bezpečnostních politikách a metodikách a spolupracovat s dalšími bezpečnostními rolemi (5).

2.13.4 Manažer kybernetické bezpečnosti

Bezpečnostní role manažer kybernetické bezpečnosti je dle VKB odpovědná za systém řízení bezpečnosti informací, za pravidelné informování vrcholného vedení o činnostech vyplývajících z rozsahu jeho odpovědnosti a o stavu systému řízení bezpečnosti informací. Bezpečnostní rolí může být pověřena osoba, která je pro tuto činnost řádně vyškolena a může prokázat alespoň tříletou praxi v oboru informační nebo kybernetické bezpečnosti nebo je absolventem studia na vysoké škole a má alespoň rok praxe v informační nebo kybernetické bezpečnosti (5).

Manažer kybernetické bezpečnosti *„nesmí být pověřen výkonem rolí odpovědných za provoz informačního a komunikačního systému“* (5).

2.13.5 Architekt kybernetické bezpečnosti

Bezpečnostní role architekt kybernetické bezpečnosti je dle VKB *„odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému“* (5).

Bezpečnostní rolí může být pověřena osoba, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti po dobu nejméně tří let, nebo po dobu jednoho roku, pokud absolvovala studium na vysoké škole (5).

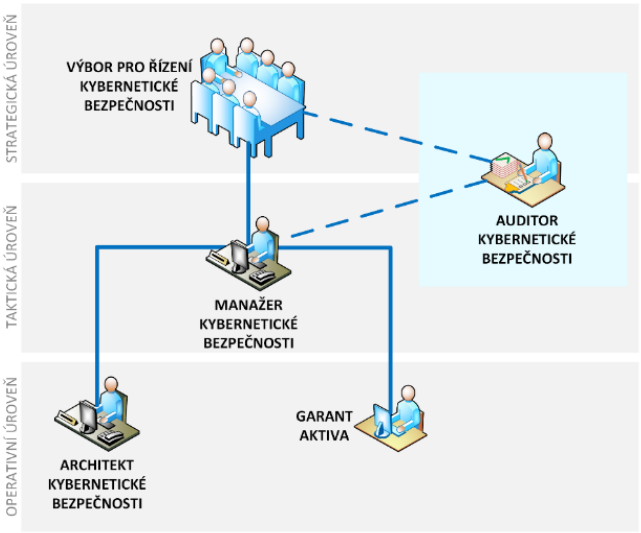
Role architekt je neslučitelná s *„rolemi odpovědnými za provoz informačního a komunikačního systému“* (5).

2.13.6 Auditor kybernetické bezpečnosti

Bezpečnostní role auditor kybernetické bezpečnosti je dle VKB odpovědná za nestranné provedení auditu kybernetické bezpečnosti (5).

Bezpečnostní rolí může být pověřena osoba, která je pro tuto činnost řádně vyškolena a je odborně způsobilá prokazatelnou praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací po dobu nejméně tří let, nebo po dobu jednoho roku, pokud absolvovala studium na vysoké škole. Auditor nesmí být pověřen výkonem jiných bezpečnostních rolí (5).

Hierarchie popsaných rolí je znázorněna na obrázku 6.



Obrázek 6: Hierarchie výboru bezpečnosti a bezpečnostních rolí (Zdroj: (25))

2.14 Základní služba

Klasifikovanou základní službou je taková služba, *„jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a narušení této služby by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura, chemický průmysl"* (15).

Informačním systémem základní služby je myšlen informační systém, na kterém je poskytování základní služby závislé. Přesné vymezení pojmu základní služba poskytuje ZKB (15).

2.15 Kritická infrastruktura

Kritickou infrastrukturu (KI) definuje *zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)*. Dle § 2 písm. g) krizového zákona (KZ) se kritickou infrastrukturou rozumí prvek KI nebo systém prvků KI, přičemž narušení jeho funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu (26).

2.15.1 Prvky kritické infrastruktury

Prvek kritické infrastruktury je vymezen KZ zejména jako stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií (26).

Určující kritéria pro prvky KI jsou stanovena *nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb. (Nařízení vlády o kritériích pro určení prvku kritické infrastruktury)* (27).

2.15.2 Průřezová kritéria

Průřezová kritéria vycházejí z *nařízení vlády č. 432/2010 Sb.,* specifikují určení KI dle výše škody.

Prvek se určí jako prvek KI dle hlediska:

- *„obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,"*
- *„ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo"*
- *„dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob"* (26).

2.15.3 Odvětvová kritéria

Odvětvová kritéria uvedena v *příloze k nařízení vlády č. 432/2010 Sb.* specifikují konkrétní odvětví zařazená do KI státu. Uvedu zde pouze relevantní kritéria pro společnost, kterou se zabývám v dalších částech této diplomové práce.

Vybraná odvětvová kritéria v rámci kategorie *energetika* jsou:

- elektřina – výrobna elektřiny, přenosová soustava, distribuční soustava,
- centrální zásobování teplem – výroba tepla, distribuce tepla (27).

Do odvětvových kritérií byla s novelou z roku 2014 (nařízením vlády č. 315/2014 Sb.) zařazena **oblast kybernetické bezpečnosti.** Opět uvádím pouze odvětvová kritéria relevantní pro tuto diplomovou práci (26).

Prvkem kritické infrastruktury v oblasti kybernetické bezpečnosti je:

- informační nebo komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,
- komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury (minimální garantovaný datový přenos 1 Gbit/s) (26).

2.15.4 Kritická informační infrastruktura

Kritickou informační infrastrukturu (KII) definuje ZKB jako *„prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti* (15).¨

Určování prvku KII probíhá podle následujícího postupu. Pokud narušení bezpečnosti informací (viz triáda CIA) posuzovaného informačního nebo komunikačního systému může mít za následek alespoň jedno z průřezových kritérií, je třeba posoudit prvek z hlediska odvětvových kritérií. Tento prvek nebo systém lze určit prvkem KII**,** splňuje-li i některé z odvětvových kritérií (28).

Určování prvků KII probíhá v součinnosti potenciálních povinných subjektů (potenciálních správců prvků KII) a zástupců NÚKIB. O konečném rozhodnutí zařazení prvku do KII je správce (případně nadřízená organizace) vždy informován (28).

2.16 Mission Critical Network

Mission Critical Network (MCN) je komunikační síť s maximální dostupností (i při poruše či havárii) s vysokými požadavky na spolehlivost, odolnost, bezporuchovost, dlouhou životnost a snadnou nahraditelnost. U sítě je vyžadován stupeň spolehlivosti, při kterém nedochází k samovolné technické poruše a který zajišťuje zachování stejných přenosových vlastností a parametrů v čase a nezávisle na prostředí.

K poruše dochází pouze v důsledku úmyslného či neúmyslného poškození některé z částí systému, kterým lze zabránit výběrem vhodných technických prostředků (v případě neúmyslného poškození) a aplikací bezpečnostních a organizačních opatření s využitím potřebných technologických prostředků (v případě úmyslného poškození). Jedná se o základní komunikační platformu kritické infrastruktury (29, s. 113).

Network Critical Physical Infrastructure (NCPI) je komplexní fyzická infrastruktura zajišťující provoz sítě MCN. Do NCPI se řadí napájení, chlazení, stojany, kabeláž, fyzická a protipožární ochrana, řídicí systémy i servis (30).

2.16.1 Specifika kritické infrastruktury v průmyslovém prostředí

Pro lepší pochopení kritické infrastruktury v průmyslovém prostředí vymezím základní pojmy související zejména se specifickým prostředím komunikační infrastruktury elektrárny, kterým se zabývá tato diplomová práce.

Komunikační infrastruktura je množina technických prostředků umožňující komunikaci jednotlivých komunikačních systémů a subsystémů. Z fyzického pohledu se

jedná o kabelážní systém pro přenos komunikací (v rámci budovy, areálu, města atd.) (29, s. 8).

Datový rozvaděč slouží k umístění přepojovacích panelů, organizérů kabeláže, aktivních prvků sítě a dalších zařízení (29, s. 19).

Páteřní vedení je sekce kabelážního systému (komunikační infrastruktury) propojující datové rozvaděče (29, s. 19).

Horizontální vedení je sekce kabelážního systému propojující datový rozvaděč se zásuvkou pracoviště (29, s. 19)..

Bezpečnostní zóna je skupina logických či fyzických aktiv sdílejících společné požadavky na bezpečnost s vytvořeným zabezpečeným spojením (31).

Spolehlivost je základní atribut pro průmyslové zařízení v sítích MCN. Požadavku na spolehlivost je podřízen celý návrh průmyslové sítě, volba systému, výběr materiálu i instalace (29, s. 113).

Spolehlivost popisují parametry:

- **MTBF** (*Mean Time Between Failures*) – střední meziporuchová doba je statistická veličina určující spolehlivost výrobku nebo výrobního zařízení. Čím je hodnota vyšší, tím je zařízení spolehlivější. Podmínkou použití této veličiny je opravitelnost výrobku či zařízení. Jednotkou MTBF je většinou rok.
- **MTTF** (*Mean Time to Failure***)** – střední doba do poruchy je statistická veličina, která se využívá k ohodnocení spolehlivosti u zařízení, která se neopravují.
- **MTTR** (*Mean Time to Restore/Recovery*) – střední doba do obnovení/zotavení je průměrná doba potřebná k navrácení zařízení (výrobku) do původního stavu. Čím je hodnota MTTR menší, tím je zařízení spolehlivější. Jednotkou MTTR je většinou hodina (29, s. 18).

Dostupnost je stěžejním parametrem určujícím provozní spolehlivost zařízení či trasy v KI**.** Používá se zejména u komunikačních systémů k vyjádření úrovně, do které je systém, popřípadě jeho součást, k dispozici a funkční. Lze ji vyjádřit jako poměr hodnoty MTBF systému vůči součtu hodnot MTBF a MTTR (29, s. 18).

Odolnost je základním atributem pro průmyslové zařízení v průmyslové části provozní technologie (OT) (29, s. 304).

Redundance neboli záložní řešení (např. komunikační trasy) je nutné pro splnění požadavku na maximální dostupnost v sítích MCN (29, s. 304).

Topologie Ring (topologie kruh) je uzavřená lineární topologie. Ke konstrukci sítě s maximální dostupností se využívá koncepce kruhové redundance. K vytvoření redundantního kruhu se využívá funkce *Ring Manager* (RM) spojující oba konce lineární páteřní struktury. V případě, že je struktura vedení neporušena RM zajišťuje uzavření redundantní linky. Dojde-li však k poruše některého ze segmentů, RM ihned otevře redundantní linku a zajistí tak funkčnost lineární struktury (29, s. 49).

OT (*Operational Technology*) *Provozní technologie*

Jedná se o technologickou síťovou infrastrukturu sloužící k monitorování a řízení výrobních procesů (13).

ICS (*Industrial Control System*) *Průmyslový řídicí systém*

Jedná se o systém řízení technologických celků, tedy obecné pojetí průmyslové síťové infrastruktury. Pod ICS spadá např. SCADA, DCS či PLC řadiče (3).

DCS (*Distributed Control System*) *Distribuovaný řídicí systém*

Jedná se o počítačový řídicí systém pro průmyslové procesy s mnoha geograficky distribuovanými (např. v továrně, stroji, kontrolní oblasti) regulačními smyčkami využívajícími autonomní řídicí systémy. Od centralizovaného řídicího systému, kde řídící funkci provádí jediný centrálně umístěný systém, se liší tím, že jednotlivé části stroje (popř. skupina strojů nebo procesní prvky) mají svůj vyhrazený vlastní řadič. Samostatně fungující řadiče jsou propojeny pomocí vysokorychlostní komunikační sítě a mají nad sebou centrální kontrolní dohled nadřazeného systému (13).

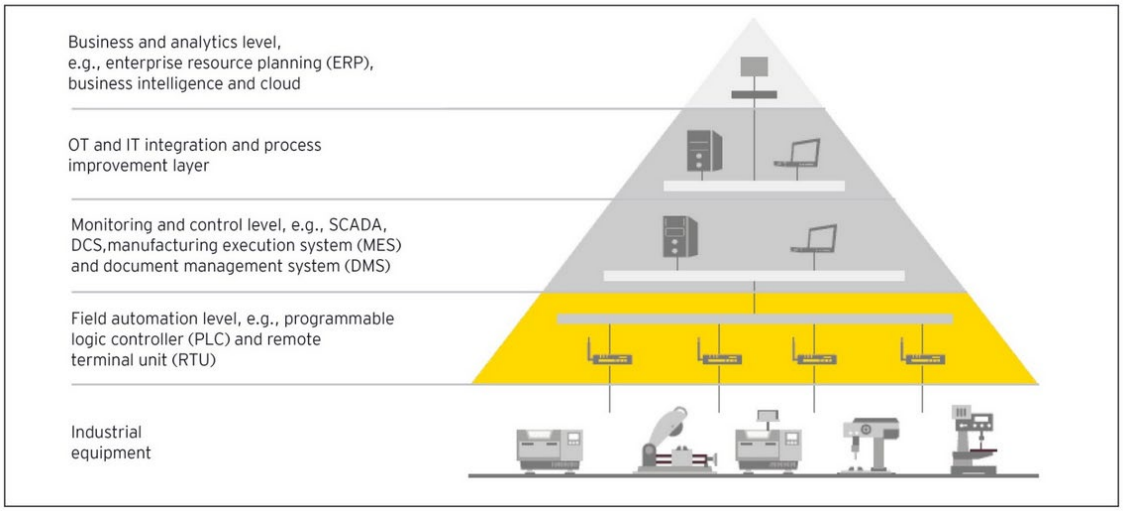
SCADA (*Supervisory Control and Data Acquisition*) *Dispečerské řízení a sběr dat*

Jedná se o dohledový a dispečerský počítačový systém pro vzdálené řízení procesů (průmyslových, infrastrukturních, procesů v zařízení) a shromažďování dat v reálném čase (3).

RTU (*Remote Terminal Unit*) *Vzdálená terminálová jednotka*

Jedná se o vzdálenou telemetrickou datovou jednotku ke sběru dat a řízení určené k podpoře vzdálených stanic SCADA a DCS. Funkci RTU v některých případech přebírá PLC zařízení, které je univerzálnější (32).

Na obrázku 7 je vidět pyramida IT a OT technologie.



Obrázek 7: Pyramida IT a OT technologie (Zdroj: (33))

Ve spodní vrstvě jsou samotná průmyslová (výrobní) zařízení (*Industrial Equipment*), na kterou navazuje specifická úroveň – field (*Field Automation Level*) s průmyslovými zařízeními s požadavky na maximální dostupnost a práci v reálném čase. Patří sem zařízení jako senzory, PLC nebo RTU. Tato úroveň používá speciální komunikační protokoly (Modbus, Profinet atd.). Dohled nad úrovní *field* zabezpečuje informační systém SCADA (*Monitoring and Control Level*). Následuje vrstva integrace a zlepšování procesů (*Integration and Process Improvement Layer*) a vrstva podnikových aplikací (*Business and Analytics Level*) (33).

Průmyslová sběrnice je fyzická síťová infrastruktura průmyslových zařízení (31).

Průmyslové protokoly jsou komunikační protokoly pro průmyslové aplikace ve smyslu aplikační sběrnice (31).

Fieldbus je datová průmyslová sběrnice sloužící k napojení senzorů a ostatních výrobních zařízení (jako převodníky, akční členy atd.) k PLC. Jedná se o skupinu protokolů ve smyslu aplikační sběrnice pro průmyslovou aplikaci (normalizováno podle IEC 61158). Sběrnicové řešení nahrazuje přímé napojení řídících jednotek s každým zařízením a komunikuje na základě příslušných protokolů. Slouží k řízení a sledování procesů v reálném čase. Příkladem tzv. Fieldbus systémů jsou **Profibus, Powerlink, Modbus.** (32).

Profibus (*Process Fieldbus*) je průmyslová sběrnice sloužící k řízení výroby a automatizaci procesů. Sběrnice Profibus je standardizovaná mezinárodní normami IEC 61158 and IEC 61784 (34).

Powerlink je průmyslová sběrnice standardizovaného systému založeného na technologii Ethernet (35).

Modbus je otevřený protokol používaný pro komunikaci různých zařízení jako jsou snímače, měniče a čidla. Využívá se k monitorování výrobních zařízení s využitím PLC, je vhodný i pro RTU. Komunikace může probíhat prostřednictvím rozhraní RS485 a RS232 (Modbus RTU) nebo TCP/IP protokol sítě Ethernet (Modbus TCP/IP) (36).

VPN (*Virtual Private Net*) je privátní počítačová síť umožňující vzdálené připojení do privátní sítě (LAN) přes prostředí veřejné sítě (Internet, WAN). Připojení je zajištěno pomocí šifrovaného tunelu. Pro ověření totožnosti obou stran při navázání spojení se využívají digitální certifikáty (3).

2.16.2 Požadavky na ICS

Základní požadavky komunikace v průmyslových sítích jsou:

- **Komunikace v reálném čase** u některých aplikací v kombinaci s deterministickým způsobem komunikace.
- **Maximální dostupnost** a **redundance**.
- **Bezpečnost protokolu** (spolehlivost) zajišťující správnou interpretaci řídicí zprávy.
- **Informační bezpečnost** zaručující původ řídicí zprávy.
- **Dlouhá životnost** komponentů.
- Zajištění **ochrany procesů**.
- Ke komunikaci se využívá **vícero protokolů** (31).

Změna priorit v triádě CIA

V průmyslovém prostředí dochází ke změně priorit v triádě CIA ve formě přeskupení důvěrnosti a dostupnosti (31). V tabulce 1 je vidět rozdíl priorit u triády CIA porovnáváme-li ICS s běžným IT systémem.

Tabulka 1: Změna priorit v triádě CIA pro průmyslové prostředí (Zdroj: Vlastní zpracování dle (31))

Priorita	IT	ICS
1	Důvěrnost	Dostupnost
2	Integrita	Integrita
3	Dostupnost	Důvěrnost

2.17 Řízení rizik

Subjekty vymezené ZKB mají povinnost řídit rizika. V souvislosti s řízením rizik je třeba vymezit základní pojmy.

Hodnocení rizik je proces identifikace, analýzy a vyhodnocení rizik (5).

Analýzu rizik definuje norma ČSN ISO/IEC 27005:2013 jako proces pochopení původu rizik a zjištění úrovně rizik. Je vstupem pro vyhodnocení rizik a následného rozhodnutí o ošetření rizik (23).

Akceptovatelné riziko je riziko, které povinná osoba dle ZKB vyhodnotí jako přijatelné bez nutnosti aplikace dalších opatření (5).

Zbytkové riziko je riziko, které přetrvává po ošetření rizika (23).

Pravděpodobnost incidentu vyjadřuje možnost výskytu incidentu (23).

Následek je výsledek po působení incidentu (23).

Úroveň rizika je velikost (míra) rizika. Stanovuje se podle zvolené metodiky hodnocení rizik. Podle ISO 27005 se vyjadřuje jako kombinace následků a pravděpodobnosti scénáře incidentu (23). Podle VKB se úroveň rizika stanoví kombinací hrozby, zranitelnosti a dopadu na aktivum (vychází z hodnoty aktiva) (23).

Ošetření rizika je proces modifikující riziko a definování plánu pro ošetření rizik (23).

Možnosti ošetření rizik jsou následující:

- **Modifikace rizika** je změna úrovně rizika formou zavedení, odstranění nebo změnou opatření, která povede k vyhodnocení zbytkového rizika za přijatelné.
- **Podstoupení rizika** se využívá, pokud úroveň rizika splňuje kritéria pro akceptaci rizik. Jedná se o rozhodnutí o přijetí rizika bez zavedení opatření.
- **Vyhnutí se riziku** spočívá ve vyhnutí se činnosti nebo jiné příčině, která umožňuje vznik rizika.

- **Sdílení rizika** je forma ošetření rizika, při které organizace sdílí riziko s externí stranou, která zvládne efektivně ošetřit riziko (23).

Plán zvládání rizik patří mezi povinnou dokumentaci dle VKB. Vymezuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, finanční, technické, lidské a informační zdroje, stanovuje časové rozvržení zavádění bezpečnostních opatření a způsob realizace bezpečnostních opatření (5).

Prohlášení o aplikovatelnosti (PoA) je jeden z povinných dokumentů podle VKB obsahující přehled bezpečnostních opatření, aplikovaných i neaplikovaných včetně odůvodnění. Vychází z výsledků analýzy rizik (5).

Řízení rizik je proces, při kterém se hodnotí rizika, vybírají a zavádějí se opatření pro zvládání rizik, sdílí se informace o riziku a následně se rizika sledují a přezkoumávají (5). Jinými slovy jde o identifikaci a kvantifikaci rizik, kterým organizace může čelit s následným stanovením způsobu zvládání těchto rizik (37, s. 95).

V oblasti ISMS se řízením rizik zabývá **norma ČSN ISO/IEC 27005** Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.

Fáze řízení rizik jsou následující:

- **Stanovení kontextu** je fáze vymezení oblasti řízení rizik, stanovení metodiky pro hodnocení rizik a kritérií pro akceptaci (zvládání) rizik, stanovení přístupu k řízení rizik, definování rolí a odpovědností a stanovení referenční úrovně (37, s. 96).
- **Analýza rizik** je fáze identifikace a hodnocení aktiv a k nim relativních hrozeb a zranitelností, identifikace stávajících opatření, spolu se stanovením úrovně rizika (37, s. 96).
- **Vyhodnocení rizik** je fáze, při které se rizika priorizují a volí se vhodná opatření za účelem snížení rizik (37, s. 96).
- **Zvládání rizik** je fáze rozhodování o optimálním způsobu zvládání rizik (37, s. 96). V této fázi se ošetřují rizika podle plánu zvládání rizik (5).
- Na základě stanovených kritérií pro akceptaci rizik (s ohledem na politiky, záměr a cíle organizace) nastává fáze **akceptace rizik**, která zahrnuje přijetí zbytkových rizik vedoucími pracovník (23).

O celém procesu řízení rizik je třeba informovat příslušné vedoucí pracovníky a zaměstnance (23).

Výstupem jednotlivých etap je rozhodnutí ve formě jednoho nebo více variant řešení. V případě, že je stanovená úroveň rizika nepřijatelná, je třeba zastavit proces a přijmout příslušná opatření ke snížení rizika. Pokud nastane situace, že zbytkové riziko nelze efektivně snížit zavedením opatření, vypracovávají se krizové plány (37, s. 96).

Řízení rizik v organizaci by se měl být nepřetržitý proces se systematickým přístupem. V rámci řízení rizik je tedy důležité **kontinuální monitorování a přezkoumávání rizik** a neustálé **zlepšování procesu řízení rizik** (23).

3 ANALÝZA SOUČASNÉHO STAVU

Analytická část poskytuje podklady pro samotnou implementaci softwarového (SW) nástroje řízení kybernetické bezpečnosti (dále jen nástroj) do společnosti. Součástí je analýza společnosti, do které je tento nástroj zaváděn, informace potřebné pro výběr vhodného nástroje, včetně následné detailnější analýzy vybraného nástroje.

Vzhledem k riziku zneužití jsou informace, které by mohly vést k identifikaci organizace anonymizovány.

Analýza a návrhová část má formu implementační dokumentace, tedy je strukturována tak, jak implementace ve firmě skutečně probíhala.

3.1 Charakteristika společnosti

V následujících podkapitolách uvádím podstatné informace o společnosti, ve které je softwarový nástroj implementován.

3.1.1 Základní informace o společnosti

Hlavní činností analyzované společnosti (elektrárny) je výroba a prodej elektřiny a tepla, včetně poskytování podpůrných služeb pro provozovatele přenosové soustavy ČEPS. K zajištění služeb elektrárna využívá parní kotle spalující uhlí, parní turbogenerátory a další související technologie (zauhlování, odsíření spalin, chemickou úpravnu vody atd.). Elektrická energie je vyvedena pomocí vysokonapěťových vedení do elektrizační soustavy ČR, tepelná energie potom pomocí horkovodních napaječů do okolních měst a obcí. Na horkovodní tepelné napaječe jsou napojeny směšovací, předávací a objektové stanice tepla, tvořící distribuční soustavu zásobování teplem. Koncovými odběrateli tepla jsou jak domácnosti, tak i průmyslové podniky a státní instituce (38).

Právní forma podniku je akciová společnost. Společnost zaměstnává 500–999 interních pracovníků (39).

Celkový finanční roční obrat organizace se pohybuje v řádu několika miliard českých korun (40).

Elektrárna usiluje o minimalizaci dopadů svých činností na životní prostředí, což potvrzuje soustavný proces certifikace podle mezinárodního standardu ČSN EN ISO 14001 v rámci auditu systému řízení životního prostředí (40).

Z hlediska kategorizace bezpečnostních rizik byl podnik určen prvkem kritické infrastruktury (KI) státu v oblasti „výroba elektřiny poskytující podpůrné služby“ (dle nařízení vlády č. 432/2010) (38).

3.1.2 Organizační hierarchie

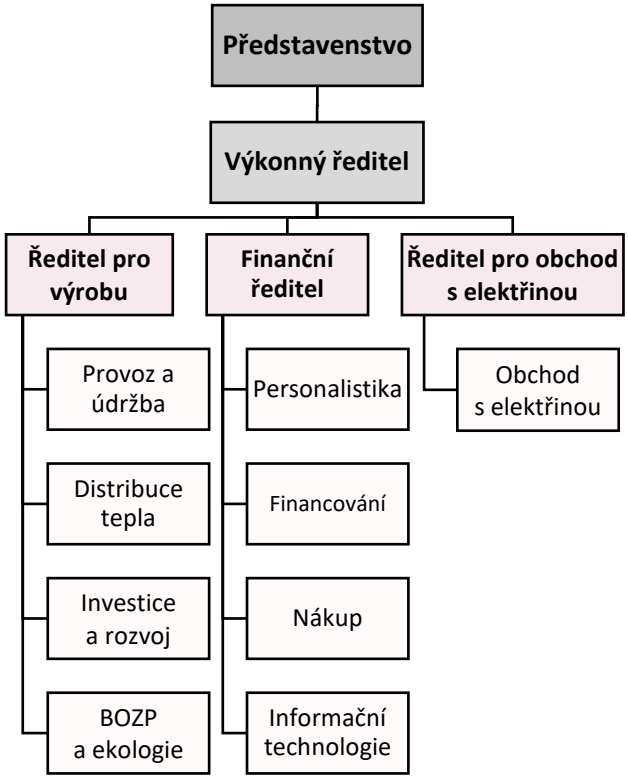
Organizační struktura společnosti vyplývá ze dvou základních faktorů:

a) jedná se o soukromoprávní akciovou společnost
b) jedná se o technologický průmyslový podnik

Výsledná organizační struktura vzniká postupně jednáním více různých vlivových skupin/subjektů (dozorčí rada, představenstvo, akcionáři, odborová organizace apod.).

Na obrázku 8 vidíme základní schéma hierarchické organizační struktury. Vrcholové orgány společnosti jsou složeny z představenstva a výkonného managementu. Vzhledem k tomu, že se jedná o akciovou společnost, kontroluje vedení společnosti dozorčí rada. Členové představenstva mohou společnost zastupovat ve všech záležitostech. Společnost zastupuje buď předseda představenstva spolu s jedním členem, popřípadě tři členové představenstva.

Důležitým aspektem organizační struktury je rozdělení do technologických celků (technologické divize) dle technické povahy jejich činnosti. Vzhledem k rozsáhlosti organizační hierarchie se při definicí odpovědností jednotlivých úseků, pozic a rolí detailněji zaměřuji pouze na ty, které jsou relevantní během implementace, respektive z hlediska řízení kybernetické bezpečnosti.



Obrázek 8: Organizační schéma elektrárny (Zdroj: Vlastní zpracování dle (38))

Výkonný ředitel přímo řídí přímé podřízené dle organizačního schématu. *Úsek ředitele pro výrobu* se dělí na několik oddělení, která jsou odpovědná za optimální pokrytí palivových potřeb společnosti, provoz a údržbu, za distribuci tepla, rozvoj podpůrných informačních technologií včetně správy smluvních vztahů, realizací schválených projektů rozvoje společnosti, dodržování obecně závazných právních předpisů a individuálních správních rozhodnutí v oblasti BOZP a ochrany životního prostředí.

Pod úsek *Finančního ředitele* spadá řízení personalistiky, účetnictví a nákupu, správa finančního plánu společnosti a jeho kontrola. Oddělení informačních technologií je zodpovědné za vytváření administrativního informačního systému, jeho provoz a údržbu zařízení dispečerské a řídící techniky.

Do oddělení informačních technologií spadá pozice s důležitou rolí v oblasti kybernetické bezpečnosti, *Architekt kybernetické bezpečnosti*, který navrhuje a implementuje bezpečnostní opatření v rámci systému řízení informační a kybernetické bezpečnosti a ochrany osobních údajů. Odpovědnost stanovuje schválená bezpečnostní politika.

Úsek ředitele pro obchod s elektřinou se zabývá řízením a koordinací obchodování s elektřinou, podpůrnými službami a emisními povolenkami.

Mezi poradní orgány výkonného ředitele patří *Výbor kybernetické bezpečnosti*, jehož předsedou je výkonný ředitel, tajemníkem je manažer kybernetické bezpečnosti (MKB) a mezi členy patří ředitel pro výrobu, vedoucí útvaru IT a architekti kybernetické bezpečnosti.

V následujících odstavcích vymezím další podstatné role a útvary společnosti.

Právní útvar poskytuje právní služby při podnikání společnosti a jejich soulad s relevantními právními normami, vyhotovuje a spravuje právní dokumenty.

Pozice *Interního auditora* má několik rolí. S jeho rolí je vázaná odpovědnost za odhalování systémových nedostatků v rámci působení společnosti. Interní auditor ověřuje dodržování pravidel stanovených představenstvem a výkonným vedením.

Další roli, kterou vykonává je role *Manažera kybernetické bezpečnosti,* ze které plyne odpovědnost za systém řízení informační a kybernetické bezpečnosti. Spolu s odpovědnými útvary a specialisty zajišťuje shodu s požadavky ZKB.

V rámci role *Koordinátora ochrany osobních údajů* řídí systém ochrany osobních údajů a spolu s odpovědnými útvary a specialisty zajišťuje shodu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, GDPR) a se zákonem č. 110/2019 Sb., o zpracování osobních údajů a souvisejících předpisů.

Role *Manažera rizik* ručí za plnění povinností stanovených politikami, implementovanými do interních norem (zejm.: politika prověřování obchodních partnerů, politika proti korupci a úplatkům, politika antimonopolního zákona, politika sankcí) (38).

3.1.3 Dodavatelé služeb

Společnost má uzavřené smlouvy s řadou dodavatelů služeb. Patří mezi ně poskytovatelé poradenských a inženýrských činností, poskytovatelé servisních služeb spočívajících v provádění oprav a kalibraci (např. odporových teploměrů a měřičů) a servisních služeb zajišťujících údržbu, opravu a rekonstrukci řídicího systému technologických uzlů soustavy distribuce tepla. Elektrárna dále využívá dodavatele energetického uhlí, mletého vápence a močoviny do sídla společnosti. Na podporu a údržbu informačních systémů najímá dodavatele IT služeb (40).

Mezi dodavatele patří také firma zajišťující implementaci vybraného softwarového nástroje řízení kybernetické bezpečnosti včetně konzultace v oblasti kybernetické bezpečnosti, kterou se dále zabývá tato diplomová práce.

3.1.4 Popis komunikační infrastruktury

V průmyslovém prostředí je bezpečnost provozu ICS klíčovým prvkem a je dosahována s využitím maximálních možností aplikovaných bezpečnostních doporučení.

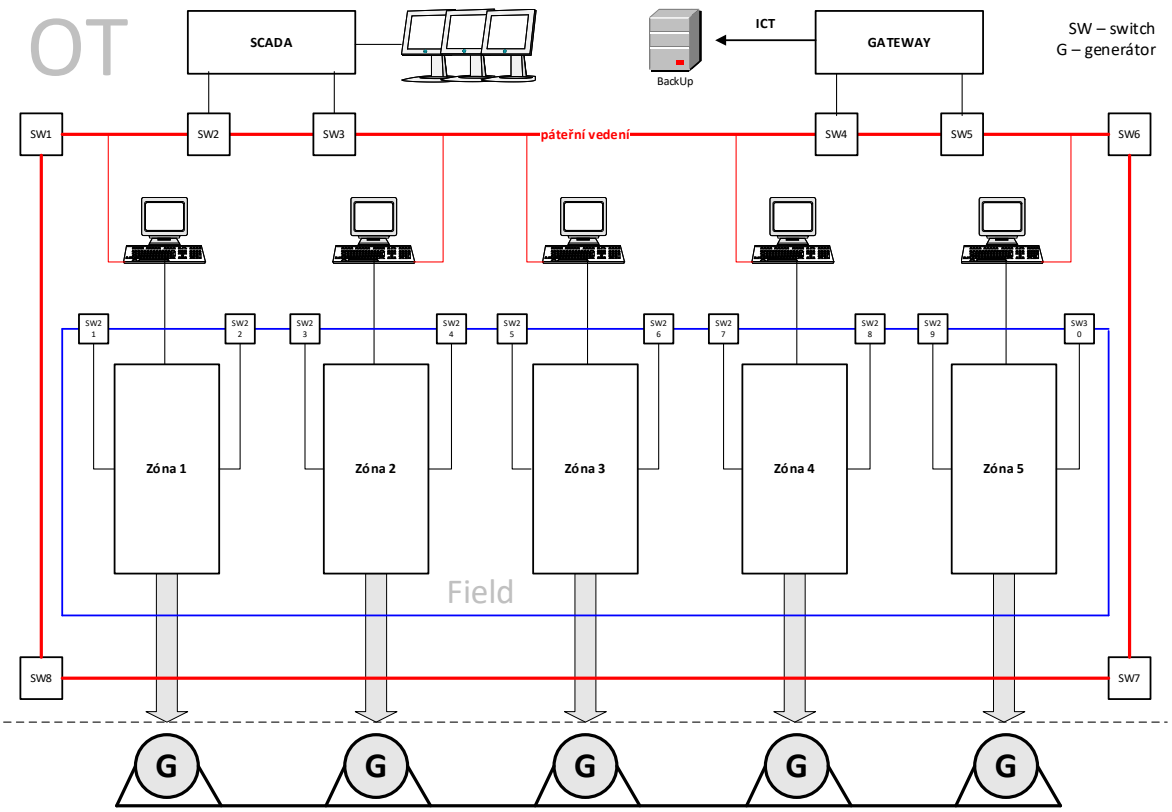
Jedním ze základních parametrů průmyslových aplikací je práce v reálném čase. Proto jsou požadavky na průmyslovou infrastrukturu specifické a v podstatě nekompromisní.

Anonymizovaný popis průmyslové infrastruktury pro dohled nad výrobou elektřiny striktně vychází z následujících mezinárodních doporučení:

- ČSN EN/IEC 62443 Bezpečnost pro systémy průmyslové automatizace a řízení,
- ČSN EN/IEC 61850 Komunikační sítě a systémy pro automatizaci v energetických společnostech,
- ČSN EN/IEC 61508 Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností (41).

Popis komunikační infrastruktury elektrárny je založený na vymezené problematice a pojmech v kapitole 2.16.1 a skutečném provedení ve výrobní části elektrárny (OT).

Zjednodušené blokové schéma OT infrastruktury elektrárny vychází z technických materiálů poskytnutých společností a je znázorněno na obrázku 9. Toto schéma stručně popisuji v následujících odstavcích.



Obrázek 9: Zjednodušené schéma OT infrastruktury elektrárny (Zdroj: Vlastní zpracování dle (38))

Páteřní vedení průmyslové komunikační infrastruktury je provedeno v topologii kruh, kde je využito topologické redundance. Na obrázku 9 je páteřní vedení vyznačeno červenou barvou.

Jednotlivá zařízení (síťové aktivní prvky) vytvářející páteřní vedení jsou zapojena jako redundantní, redundance je dosaženo zapojením více než jednoho zařízení se stejnou funkcionalitou.

Jednotlivé zóny jsou opět propojeny v redundantní topologii kruh (na obrázku modře). Připojení k páteřnímu vedení je realizováno redundandně pomocí dvou zařízení. Zónové aktivní prvky pro řízení průmyslových zařízení jsou v základním zapojení zdvojeny.

Dohled a správu OT infrastruktury v reálném čase zabezpečuje dohledový a dispečerský informační systém SCADA. V části infrastruktury pro připojení průmyslových zařízení (na obrázku označeno *Field*) jsou použity průmyslové sběrnice Powerlink, Modbus a Profibus (v závislosti na konkrétním zařízení a doporučení výrobců těchto zařízení). Tomu odpovídají použité komunikační protokoly.

Použitá zařízení v OT infrastruktuře splňují požadavky na průmyslové řešení z hlediska spolehlivosti (podle parametrů MTBF a MTTR) a odolnosti (zodolněná zařízení pro náročná provozní prostředí z pohledu teploty, prašnosti, a především elektromagnetického rušení).

Externí správa jednotlivých průmyslových zařízení nebo technologických celků je řešena zabezpečeným připojením pomocí VPN.

Zálohování dat je realizováno „externě“ v ICT infrastruktuře elektrárny připojenou přes redundandně zapojenou bezpečnostní bránu (Gateway). Na této bráně jsou také nastavena pravidla povolené komunikace mezi sítěmi IT a OT.

3.2 Požadavky zadavatele

Pro správný výběr nástroje je třeba identifikovat požadavky a objasnit si povinnosti vyplývající pro analyzovaný subjekt z VKB. Zadavatelem je výbor kybernetické bezpečnosti v zastoupení manažera kybernetické bezpečnosti (MKB).

Velmi důležité je stanovit si klíčové uživatele nástroje. Těmi budou manažer kybernetické bezpečnosti (MKB) a garanti aktiv. Výstupy nástroje musí být **srozumitelné a přijatelné pro externí auditní tým.**

Ve spolupráci se zadavatelem byly definovány následující požadavky pro výběr nástroje:

- **Soulad s legislativou** – soulad s VKB a normami ISMS (normy řady ISO/IEC 27000).
- **Efektivita řízení** – efektivní systémové řízení procesů, které splňuje požadavky řízení kybernetické bezpečnosti.
- **Optimalizace** – nahrazení nedostatku lidských zdrojů v organizaci optimalizací procesů.
- **Automatizace řízení** – automatizovaná analýza rizik postavená na řízení aktiv s reálným dopadem a výběrem opatření.
- **Výstupy** – součástí výstupní dokumentace nástroje bude zpráva o hodnocení aktiv, analýza rizik, prohlášení o aplikovatelnosti (PoA).
- **Specializace na průmyslové systémy –** výhodou je uzpůsobení SW pro potřeby průmyslového (KII) prostředí.
- **Způsob implementace a zálohování** – on-premise software.

- **Jazyk** – nástroj i výstupní dokumentace musí být v českém jazyce.
- **Uživatelé** – možnost zřízení individuálních uživatelských účtů s definovanými rolemi.
- **Ochrana osobních údajů** – nástroj umožňující do budoucna také soulad s GDPR výhodou.
- **Uživatelská podpora** – podpora (maintenance, helpdesk) ze strany dodavatele nástroje.
- **Cena** – nízká cena licence a implementace výhodou.

3.3 Legislativní rámec

Na chod společnosti má vliv zejména následující legislativa:

- *zákon č. 458/2000 Sb.., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon),* ve znění pozdějších předpisů, a další související zákony (42),
- *zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)* ve znění pozdějších předpisů – definuje kritickou infrastrukturu (KI), upravuje ochranu KI (práva a povinností při přípravě na krizové situace) (26).

Analyzovaná společnost splňuje kritéria pro určení prvku kritické infrastruktury, není určena povinným subjektem spadající do kategorie subjektů zajišťujících základní službu (ZS).

Legislativa pro určení prvků KI:

- *nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury* ve znění pozdějších předpisů – kapitola I. ENERGETIKA – stanovuje kritéria určující prvky KI (16).

Z hlediska kybernetické bezpečnosti je důležitá následující legislativa upravující přímo bezpečnostní politiky společnosti:

- *zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* ve znění pozdějších předpisů – definuje povinné subjekty, na které se zákon vztahuje a ukládá jim povinnosti (dále jen ZKB),

- *vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti* ve znění pozdějších předpisů – upřesňuje bezpečnostní opatření požadovaná po KII (dále jen VKB) (16).

Legislativa upravující zpracování osobních údajů:

- *nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),*
- *zákon č. 110/2019 Sb. (zákon o zpracování osobních údajů)* (43).

Výkonnou složkou dozoru nad společností v oblasti kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Mezinárodní bezpečnostní norma pro energetický průmysl:

- *ČSN EN ISO/IEC 27019:2017 Informační technologie – Bezpečnostní techniky – Opatření bezpečnosti informací pro energetický průmysl* (41).

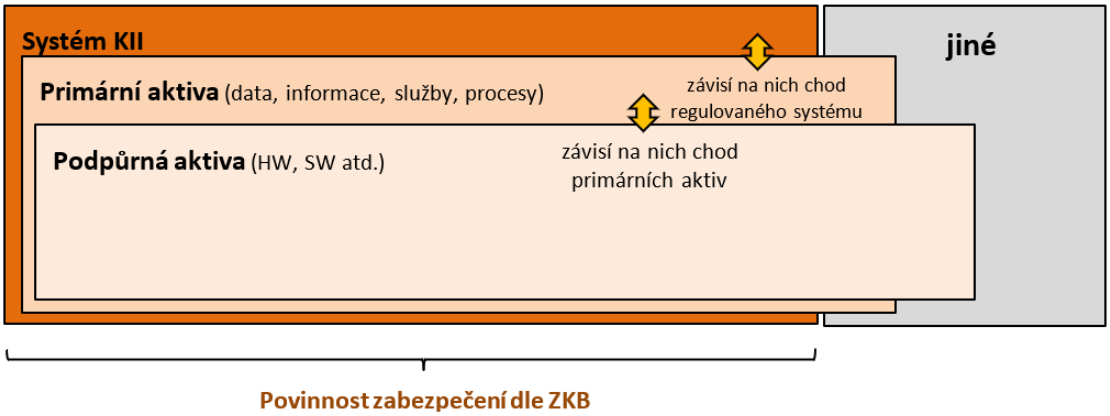
3.4 Rozsah ISMS

Pro účely implementace je třeba stanovit rozsah ISMS. Primárně je rozsah určen výše zmíněnou legislativou v oblasti kybernetické bezpečnosti (VKB a ZKB).

Sekundárně je rozsah vymezen aktivy. Vzhledem k tomu, že bude elektrárna (na výzvu NÚKIB) pravděpodobně subjektem povinným dle ZKB z titulu zařazení do tzv. „kritické informační infrastruktury“ (KII), bude společnost povinna zabezpečit primární a podpůrná aktiva, na kterých je závislý chod regulovaného systému KII.

Rozsah a hranice identifikace a hodnocení aktiv se stanovují se zohledněním činností a procesů, které jsou důvodem pro zařazení elektrárny do prvků KII. Naopak zabezpečení aktiv, která nemají vliv na regulovaný systém ZKB nevyžaduje.

Vymezení obecného rozsahu regulovaného systému je graficky znázorněno na obrázku 10.



Obrázek 10: Vymezení regulovaného systému dle ZKB (Zdroj: Vlastní zpracování dle (44))

U elektrárny je rozsah primárně vymezen systémy, které reguluje ZKB a závisí na nich následující procesy:

- výroba elektřiny a poskytování podpůrných služeb,
- výroba tepla,
- distribuce tepla.

Minimální rozsah identifikace a hodnocení aktiv je definován primárními a podpůrnými aktivy, které jsou součástí výše uvedených procesů.

Elektrárna je v současné době určena prvkem kritické infrastruktury státu v oblasti „výroba elektřiny poskytující podpůrné služby“ opatřením obecné povahy. Dosud nebyla určena prvkem kritické infrastruktury ani dodavatelem základní služby v oblasti výroby a distribuce tepla.

Po dohodě se zadavatelem i vzhledem k výše uvedenému byl rozsah v úvodní fázi zúžen na primární aktivum:

- **výroba elektřiny a poskytování podpůrných služeb**.

Dále byl rozsah implementace zadavatelem zúžen na vstupní analýzu rizik, tj. pouze prvotní analýza (ne)zavedených opatření.

3.5 Výběr vhodného nástroje

Na základě požadavků zadavatele provedu výběr vhodného SW nástroje pro řízení kybernetické bezpečnosti. Informace pro analýzu nástrojů byly čerpány z oficiálních webových stránek, z volně dostupných materiálů a produktových listů k nástrojům obdržených na vyžádání.

Vzhledem k poměrně malé nabídce tohoto typu nástrojů byly do výběru zahrnuty tři nástroje nejlépe vyhovující požadavkům. Výběr byl zúžen pouze na nástroje s podporou českého jazyka a české legislativy. Předpokládá se, že každý z nástrojů je schopen dostát požadavkům na zvýšení efektivity řízení kybernetické bezpečnosti a požadavku optimalizace lidských zdrojů.

Nástroje stručně představím a následně je zhodnotím podle míry splnění požadavků zadavatele.

ESKO CZ KBO je podpůrný nástroj pro proces řízení kybernetické bezpečnosti v organizaci. Architektura nástroje je typu klient-server. Jedná se o nástroj slovenského dodavatele ISIT Slovakia přizpůsobený pro české právní prostředí. Vychází také z norem normy ISO 27000. Výhradním distributorem v České republice je společnost Sevitech (45). Součástí nástroje jsou vzory smluv a kompletní bezpečnostní dokumentace. Modul KBO lze rozšířit o GDPR modul s posouzením vlivu na ochranu osobních údajů – DPIA (*Data Protection Impact Assessment*). Nástroj poskytuje možnost výběru typu organizace (včetně KII). Na základě výběru poskytuje specifické hrozby, zranitelnosti a opatření namapované k jednotlivým aktivům. Mezi další funkcionality nástroje patří řízení incidentů včetně generovaného hlášení příslušným autoritám a možnost provádění automatizovaných interních a externích auditů. Při zakoupení licence poskytuje dodavatel nástroje maintenance a helpdesk (46).

Gordic CyberSec (CSA) je nástroj pro řízení kybernetické bezpečnosti vyvinutý v České republice společností Gordic. Jedná se o webovou aplikaci s vícevrstvou architekturou. Nástroj vychází z příslušné české legislativy doplněné o zapracované specifické materiály od NÚKIB a doporučení norem ISO 27000. Jedná se o webovou aplikaci hostovanou na cloudové platformě Microsoft Azure. Výstupní materiály jsou v souladu s požadavky dozorových orgánů. Nástroj CSA je možné propojit s aplikací GDA pro komplexní zprávu GDPR. Součástí je možnost provedení automatizovaného auditu (47).

Zoty je nástroj od společnosti IDS Advisory pro implementaci integrovaného systému řízení rizik včetně těch kybernetických. Jedná se o uživatelsky konfigurovatelnou webovou aplikaci, která nabízí různé metodické přístupy k řízení rizik (včetně kybernetických) obohacené o best practice. Podporuje snadnou integrovatelnost prostřednictvím konceptu otevřeného API rozhraní. V nástroji je možné modifikovat způsob hodnocení pomocí konfigurovatelných schémat. Je v souladu s českou legislativou a aplikuje i normy ISO 27000 (48).

Shrnutí hlavních požadavků zadavatele a jejich naplnění je v následující tabulce 2. Pro hodnocení je stanovena stupnice 0–10, kdy 0 značí naprosté nesplnění požadavků (případně informaci nešlo z dostupných zdrojů získat) a 10 úplné splnění požadavků. Při neúplném splnění požadavků se odečítá adekvátní množství bodů od hodnoty 10.

V tabulce je uvedeno devět požadavků zadavatele, a tedy maximální možné hodnocení je **90 bodů**. Vybrán bude nástroj s nejvyšším hodnocením.

Tabulka 2: Srovnání softwarových nástrojů s hodnocením (Zdroj: Vlastní zpracování dle (45), (47), (48))

NÁSTROJ		ESKO CZ KBO		Gordic CyberSec (CSA)		Zoty	
POŽADAVKY		**POPIS**	**HODNOCENÍ**	**POPIS**	**HODNOCENÍ**	**POPIS**	**HODNOCENÍ**
	Auditní nástroj	ano	**10**	ano	**10**	ano	**10**
	Soulad s legislativou	splňuje požadavky ZKB a VKB, GDPR, řada norem ISO 27000	**9**	splňuje požadavky ZKB a VKB, GDPR, řada norem ISO 27000, materiály NÚKIB	**10**	splňuje požadavky ZKB a VKB, řada norem ISO 27000	**8**
	Automatizace	automatizovaná AR (vazby mezi zranitelnostmi – hrozbami – opatřeními), best practice	**10**	automatizovaná AR bez předdefinovaných vazeb	**8**	automatizovaná AR bez předdefinovaných vazeb, best practice	**9**
	Výstupní dokumentace	PoA, zpráva z analýzy rizik (na webu uvedeny příklady dokumentace)	**10**	PoA, zpráva z analýzy rizik, plán zvládání rizik	**9**	neuvedeno	**0**
	Specializace na průmyslové systémy (KII)	možnost výběru specifických kritérií (pro kritickou infrastrukturu, průmyslová prostředí i přímo energetiku)	**10**	neuvedeno	**0**	neuvedeno	**0**
	Implementace	on-premise	**9**	cloudové řešení	**5**	cloudové řešení, on-premise	**10**
	Uživatelská podpora	Helpdesk externí a interní (team viewer), maintenance	**10**	neuvedeno	**0**	helpdesk, maintenance	**10**
	Cena single-tenantní licence (bez DPH/rok)	jasně uvedená cena, 1 licence libovolného modulu je 1000 euro	**10**	pouze na vyžádání v závislosti na customizovaném řešení, na vyžádání nebyl sdělen ani rámcový odhad	**0**	jasně uvedená cena, 38 500 Kč	**9**
	Cena maintenance (bez DPH/rok)	první rok v ceně licence, další roky 10 % z pořizovací ceny	**10**	neuvedeno	**0**	zahrnuto v ceně roční licence	**10**
	CELKEM		**88**		**42**		**66**

3.5.1 Zhodnocení výběru

Z analyzovaných nástrojů byl nejlépe ohodnocen nástroj ESKO CZ KBO (88 bodů z 90), dále jen ESKO. Mezi hlavní výhody nástroje ESKO patří možnost specializace na průmyslové systémy včetně systémů KII. Oproti ostatním nástrojům poskytuje v rámci analýzy rizik předdefinované vazby aktivum – hrozba – zranitelnost – opatření. Výstupní bezpečnostní dokumentace se skládá ze stejných dokumentů jako u konkurenčních nástrojů, výhodou ovšem je, že jsou na webových stránkách uvedeny příklady dokumentace (např. PoA). Díky tomu si může zadavatel ověřit, zda je dokumentace vyhovující. Nástroj aplikuje postupy best practice, což je přidaná hodnota oproti požadavkům zadavatele. Současně poskytuje požadovanou možnost napojení na modul GDPR. Mezi další výhody patří transparentnost při uvádění ceny za produkt i ceny za uživatelskou podporu. Značnou výhodou je také samotná výše ceny (nejnižší z analyzovaných nástrojů). ESKO poskytuje podporu v podobě helpdesku i maintenance (údržbu) v ceně zakoupené licence (46).

Výsledky analýzy byly předloženy zadavateli, který odsouhlasil výběr nástroje ESKO a schválil koupi licence. V České republice je pouze jeden výhradní distributor ESKO softwaru, kterým je společnost Sevitech. Licence nástroje byla koupena prostřednictvím tohoto dodavatele.

3.5.2 SWOT analýza

Pro přehlednější zhodnocení nástroje ESKO, který bude následně implementován, využiji analýzu SWOT (tabulka 3). Analýza identifikuje silné stránky nabyté implementací nástroje, slabé stránky, které by mohly vést ke zpochybnění vhodného výběru nástroje, externí příležitosti pro společnost plynoucí z implementace a vnější hrozby ovlivňující samotný úspěch implementace.

Tabulka 3: SWOT analýza implementace softwaru ESKO (Zdroj: Vlastní zpracování dle (46))

	POMOCNÉ	ŠKODLIVÉ
VNITŘNÍ PROSTŘEDÍ	**Silné stránky** ● využití „best practice" ● specifikace kritérií (pro KI, KII, MCN, energetika) ● nízká cena licence ● zajištění stále aktuálního souladu s legislativou ● provádění interních auditů ● možnost pomocí dotazovacího formuláře polo-automatizované vyplnění modulu řízení aktiv pomocí ● využití vazeb hrozba – zranitelnost – opatření – aktiva ● možnost školení a eLearning pro uživatele v oblasti kybernetické bezpečnosti ● správa dokumentů ● využití poradenství ● automatizované vytvoření bezpečnostní dokumentace ● možnost řízení procesů kybernetické bezpečnosti a ochrany osobních údajů/GDPR	**Slabé stránky** ● neuspokojivá vizuální stránka aplikace implementovaného nástroje ● neuspokojivá uživatelská přívětivost (neintuitivnost) implementovaného nástroje ● není poskytnuto cloudové řešení
VNĚJŠÍ PROSTŘEDÍ	**Příležitosti** ● shoda s legislativou po zařazení do prvků KII ● úspěšný audit kybernetické bezpečnosti NÚKIB	**Hrozby** ● konkurenční nástroje, které lákají na přívětivější uživatelské prostředí ● pomalá reakce na změnu legislativy ● špatná implementace externím dodavatelem služeb ● koronavirová pandemie

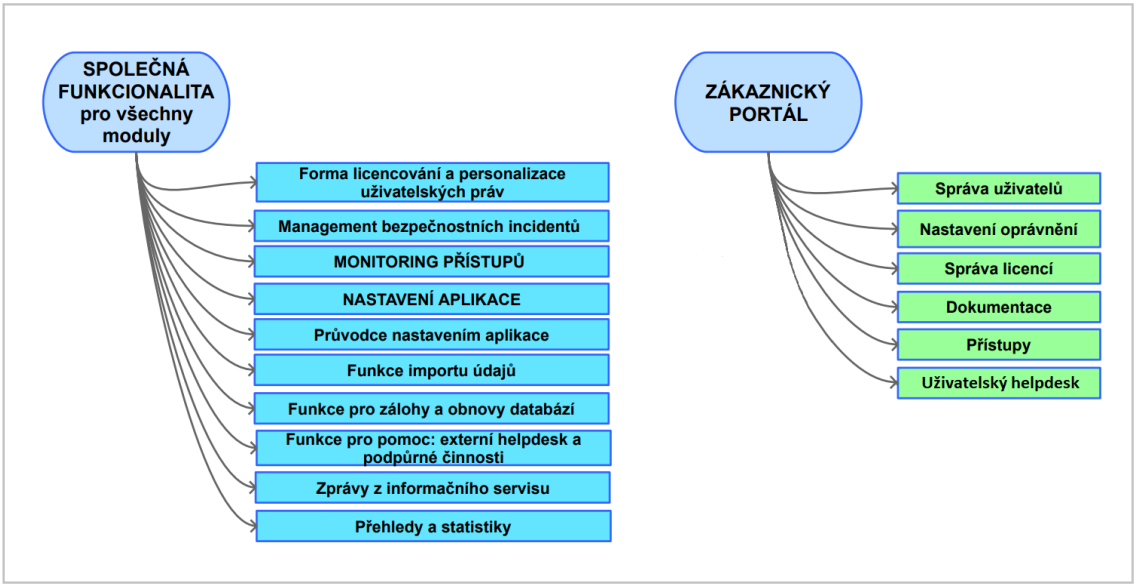
3.6 ESKO CZ

Softwarový nástroj *ESKO CZ* je automatizovaný nástroj pro podporu managementu kybernetických rizik. Jedná se o znalostní modulovou aplikaci s lokalizací v českém, slovenském a anglickém jazyce. Nástroj lze využít v malých a středních organizacích k zefektivnění ochrany informačních systémů vůči kybernetickým hrozbám a ochrany osobních údajů. Nástroj usnadňuje pracovníkům v organizaci, kteří se základním způsobem orientují v problematice kybernetické bezpečnosti a ochrany osobních údajů, zajištění souladu s příslušnou platnou legislativou (46).

Software je tedy určen povinným osobám (organizacím), stanoveným příslušnou legislativou (ZKB, VKB), kteří se podílejí na procesech řízení kybernetické a informační bezpečnosti.

3.6.1 Hlavní moduly nástroje

Nástroj má dva základní moduly, jejichž společná funkcionalita je zobrazena na obrázku 11. V následujících podkapitolách rozeberu základní funkcionality obou modulů.



Obrázek 11: Společná funkcionalita modulů KBO a GDPR (Zdroj: (49))

Modul GDPR s vazbami posouzení DPIA (GDPR DPIA)

Modul *GDPR DPIA* pomáhá organizaci udržovat soulad s *GDPR* a *zákonem č. 110/2019 Sb., o zpracování osobních údajů.* Součástí modulu je i posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (*Data Protection Impact Assessment*, DPIA), řízení bezpečnostních incidentů, posouzení dopadů pro jednotlivé zpracovatelské činnosti dle účelů zpracování, evidence informačních aktiv včetně klasifikace a určení vlastníků, identifikace hrozeb, rizik, zranitelností a dopadů, evidence souhlasů subjektu údajů, analýza s generováním příslušných dokumentů a evidence kamerových systémů využívaných společností. Modul také umožňuje automatizovaný interní a externí audit ochrany osobních údajů (46).

Výstupy (sestavy) z modulu jsou následující:

- záznam o zpracovatelských činnostech,
- záznam o poučení oprávněné osoby,
- hromadný záznam o poučení oprávněné osoby,
- souhrnná evidence záznamů incidentu,
- hlášení na Úřad pro ochranu osobních údajů,
- export údajů – vazby posouzení dopadů (46).

Modul rovněž poskytuje vzory bezpečnostní dokumentace např. vzory souhlasů subjektu údajů, pověření oprávněných osob, smlouvy se zprostředkovateli, záznamy o likvidaci osobních údajů a další vzory dokumentů (46).

Modul kybernetické bezpečnosti organizace

Dalším modulem je modul *Kybernetické bezpečnosti organizace (KBO).* V diplomové práci se zabývám pouze implementací KBO modelu, a proto se zaměřuji na jeho důkladnější analýzu.

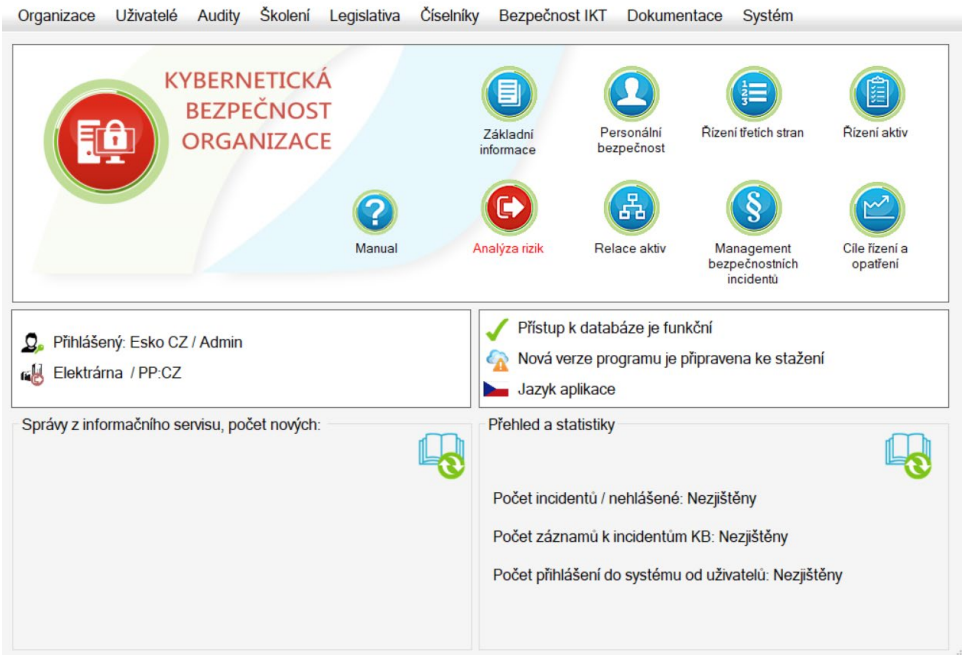
Součástí modulu je možnost využít defaultní automatizované nastavení, které umožní běžným organizacím pokrýt většinu požadavků stanovených příslušným legislativním rámcem (soulad s požadavky ZKB a VKB). Při využití modulu u společností se specifickými požadavky a při použití specialistou na kybernetickou bezpečnost lze defaultní hodnoty polo-automatizovaných funkcí měnit dle potřeby. Program je tedy škálovatelný jako konzola pro manažera kybernetické bezpečnosti (MKB) a zároveň slouží jako komplexní řízení kybernetické bezpečnosti se zapojením všech vlastníků

aktiv, rizik až po řídící složky (admin/klient). Každému uživateli jsou v rámci modulu stanoveny jeho role, na jejichž základě je uživateli uděleno oprávnění přístupu k jednotlivým funkcionalitám (49).

V aplikaci lze volit ze tří bezpečnostních modelů – podle vyhlášky kybernetické bezpečnosti č. 82/2018 Sb., podle základních pravidel KB a nejlepší praxe (best practice) a kombinace obou modelů (podrobněji rozebráno v kapitole 3.6.4).

Využití nástroje je závislé na jeho naplnění potřebnými daty získanými od zadavatele a garantů aktiv. Díky těmto datům lze následně vyhotovit analýzu rizik, která poskytne seznam aplikovaných bezpečnostních opatření a seznam opatření, která je třeba aplikovat k dosažení požadované úrovně zabezpečení systému před definovanými hrozbami. Tato navrhovaná opatření v polo-automatizovaném režimu garantují zajištění dosažení minimální úrovně zvoleného stupně zabezpečení systému. Lze zvolit úroveň – základní, standardní a zvýšené bezpečnosti. Modul KBO také poskytuje informace o jednotlivých zranitelnostech identifikovaných aktiv, hrozbách působících na konkrétní aktivum a na ně navázaných opatření. Pomocí nástroje lze generovat a uchovávat dokumenty potřebné pro audit kybernetické bezpečnosti (49).

Na obrázku 12 je vidět hlavní menu modulu KBO.



Obrázek 12: Hlavní menu modulu KBO (Zdroj: Nástroj ESKO)

V následujících odstavcích uvádím základní popis funkcionalit modulu KBO, ke kterým přiřazuji příslušné paragrafy z VKB. V případě, že se název modulu liší od přiřazeného paragrafu VKB, uvádím i upřesnění názvu dle VKB. V **příloze 1** této diplomové práce je graficky znázorněno logické uspořádání modulu. Položky základního výběru modulu jsou očíslovány. Pod položkami základního výběru jsou zařazeny jednotlivé záložky modulu.

Funkcionality modulu KBO jsou následující:

1 Audity

Management auditů

Tato záložka slouží k evidenci realizovaných interních i externích auditů.

RASCI

Jedná se o možnost záznamu matice odpovědností RASCI v rámci identifikace a hodnocení aktiv s možností jejího exportu do souboru programu Excel.

Audit cílů a opatření

Jde v podstatě o check-list cílů a jednotlivých opatření přílohy A normy ISO/IEC 27001 určený pro interní, popřípadě externí auditory (49).

2 Školení

Vzory pro oprávněné osoby

Záložka obsahuje vzory školení pro uživatele v oblasti kybernetické bezpečnosti.

eLearning

Záložka nabízí možnost připojení se na eLearning, kam lze vložit školící a testovací materiály pro zaměstnance v rámci budování bezpečnostního povědomí (49).

3 Legislativa

Tato možnost základního výběru modulu obsahuje výpis platné legislativy na území ČR, SR a mezinárodní legislativy v oblasti informační a kybernetické bezpečnosti (49).

4 Číselníky

Jedná se o možnost ze základního výběru modulu obsahující naplněné číselníky vztahující se k personální bezpečnosti, třetím stranám, jednotlivým prvkům

bezpečnosti, procesům a službám, se kterými pracuje a doplňuje je uživatel nástroje (49).

5 Bezpečnost IKT

Základní informace IS

Součástí této záložky je volba bezpečnostního modelu, kategorizace informačního a komunikačního systému, klasifikace primárních aktiv, výběr stupně bezpečnostních opatření, přiřazení privilegovaných rolí a uživatelů, seznam třetích stran, doplňující údaje a z nich generované výstupy.

Bezpečnost lidských zdrojů (VKB §9)

Do záložky se zapisují komplexní údaje o zaměstnancích z pohledu bezpečnosti, záznamy o školení zaměstnanců a jejich procesní role a odpovědnosti, záznamy o svěřených aktivech a svěřených přístupech, přesuny práv, kontroly a hodnocení. Data lze exportovat individuálně pro každého zaměstnance.

Řízení třetích stran (Řízení dodavatelů § 8)

V záložce se zaznamenávají základní údaje o třetích stranách, ustanovení o dodržování bezpečnostní politiky třetí stranou včetně možnosti vložení smlouvy, specifikace a rozsah bezpečnostních opatření, rozsah činností, personální bezpečnost třetí strany, řízení přístupů zaměstnanců třetí strany k aktivům, kontrolní činnosti, ustanovení o způsobu a formě hlášení informací požadovaných provozovatelem ICT, ustanovení o sankčních mechanismech při porušení smlouvy, podmínky pro ukončení smlouvy, postupy po ukončení smlouvy a postoupení licenčních práv po ukončení smluvního vztahu. Součástí modulu je možnost vložení příslušných dokumentů, přímého odeslání e-mailu MKB a exportu záznamů o třetí straně.

Dotazovací formulář

Jedná se o volitelnou funkci pro malé a střední organizace, která má pomoci při určování nezbytných informací pro kybernetickou a informační bezpečnost. Ve formuláři se z jednotlivých možností vybírají koncepty a postupy, které má organizace povinnost zajišťovat, povinnosti organizace ve věci zabezpečení pracovních prostorů. Obsahuje také otázky k provozním úkonům, k problematice detekce a reakce na bezpečnostní incidenty a ke složitosti IS. Výstupem z dotazovacího formuláře je přiřazení identifikovaných aktiv do modulu řízení aktiv.

Seznam aktiv (Řízení aktiv § 4)

V této části se identifikují třídy aktiv nebo konkrétní aktiva s podrobnou specifikací z pohledu základního dělení na primární a podpůrná aktiva. V modulu lze vyexportovat seznam evidovaných aktiv.

Řízení aktiv (§ 4)

V této záložce je možné ke každé třídě aktiv nebo konkrétnímu aktivu dané třídy provést popis, detailizaci, evidenci vlastníků tříd podpůrných aktiv, personálií (osoby odpovědné za evidenci, realizaci bezpečnostních opatření a správu tříd podpůrných aktiv), hodnocení tříd aktiv (stupeň důležitosti) a jejich lokaci. Obsahuje možnost exportu záznamu řízení aktiv. Klasifikace aktiv v tomto modulu je základem pro následující analýzu rizik.

Analýza rizik (§ 5 Řízení rizik)

Jedná se o automatizovanou analýzu rizik (AR). Předpokladem úspěšnosti je naplnění předchozích záložek týkajících se personální bezpečnosti, třetích stran a aktiv.

Součástí automatizované analýzy rizik je:

- parametrizace bezpečnostního modelu podle pravidel nejlepší praxe (best practice), ZKB a VKB a některých doporučení norem ISO/IEC 27000;
- podrobný popis třídy aktiva nebo aktiv včetně klasifikace;
- identifikace a klasifikace hrozeb a zranitelností;
- katalog rizik prezentovaný jako ucelený přehled, kde je určeno jednoznačné ID každého rizika přiřazeného ke konkrétnímu aktivu, jeho hrozbám a každé hrozbě s přiřazením zranitelnosti s určením a upřesněním dopadu narušení základních bezpečnostních atributů (C, I, A);
- řízení rizik (detailizované řešení ve vztahu ke konkrétnímu ID rizika, akceptace rizika, vyhnutí se riziku či sdílení rizika;
- vyhodnocení rizik (podrobné přehledy rizik s volbou mezi nezavedenými/zavedenými opatřeními);
- přijetí (akceptace) rizik;
- monitorování rizik s následným přezkoumáním.

V modulu lze provést export seznamu aktiv, hrozeb, zranitelností a export seznamu opatření.

Relace aktiv

Záložka nabízí možnost namapování vlastních relací aktiv, hrozeb, zranitelností a opatření.

Řízení bezpečnostních incidentů (část třetí VKB)

Jde o komplexní řízení incidentů. Součástí je možnost záznamu životního cyklu každého bezpečnostního incidentu od zaznamenání jeho vzniku, podrobné identifikace, řešení, až po nápravná opatření s výstupem na kontrolní orgány – NÚKIB nebo CSIRT.

Řízení kontrol dodržování bezpečnostní politiky (§ 30)

Záložka poskytuje záznamový formulář ke všem provedeným kontrolám dodržování bezpečností politiky (49).

6 Dokumentace – tiskové výstupy

Možnosti výstupní dokumentace jsou následující: export záznamů základních informací, personální bezpečnosti, třetích stran a řízení rizik; seznam aktiv AR, hrozeb AR, zranitelností AR a opatření AR; export RASCI; export tabulky – cíle řízení a opatření; souhrnná evidence záznamu k incidentu; hlášení na dozorčí orgán; výstupní zprávy o bezpečnosti IS, závěrů z řízení aktiv a analýzy rizik zkoumaného IS; prohlášení o aplikovatelnosti (PoA); legislativní východiska, použitá metodika analýzy rizik; bezpečnostní politika (49).

7 Systém

Import údajů

Tato záložka umožňuje importovat data z externích databází mzdových a personálních programů a z externích systémů prostřednictvím programu Excel.

Záloha a obnova databáze

V této záložce je možné zálohovat databáze, vybírat ze záloh a vytvářet zálohy ke konkrétnímu datu.

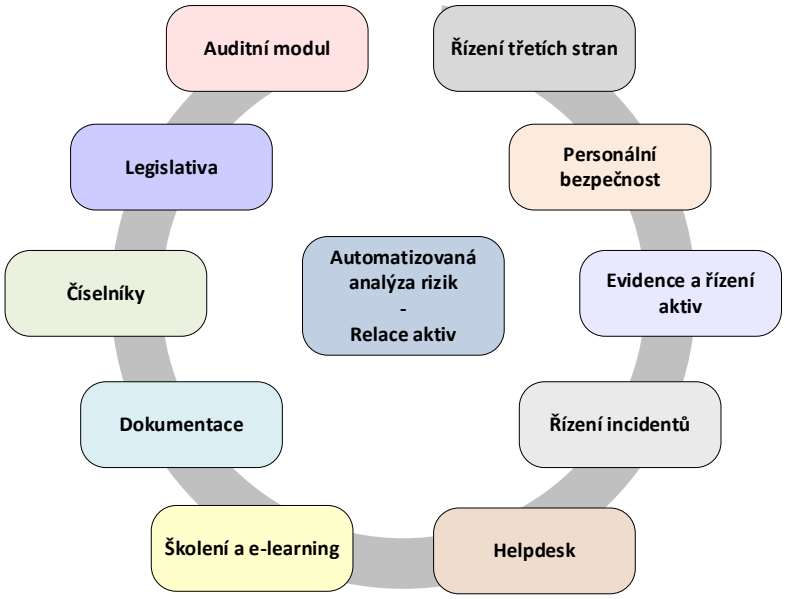
Licencování

Jde o vrstvenou správu uživatelů softwaru – multilicence s (ne)omezeným množstvím správců nebo samostatné licence. V záložce lze také spravovat uživatelské účty a jejich oprávnění přístupu k jednotlivým částem aplikace.

Uživatelský Helpdesk

Důležitou součástí nástroje pro řízení kybernetické bezpečnosti je plně samostatný uživatelský helpdesk v odpovídajícím režimu (24x365). V modulu Helpdesk jsou umístěny podpůrné materiály k nástroji, kontakty na zákaznickou podporu. Technická podpora se provádí přes Team Viewer. Součástí jsou také opravné balíčky pro tiskové sestavy a databáze Microsoft Access (49).

Na obrázku 13 jsou graficky znázorněny moduly SW nástroje.



Obrázek 13: Modularita SW nástroje (Zdroj: (50))

3.6.2 Licenční podmínky a specifikace licencí

Pro malou firmu většinou postačuje jedna administrátorská licence (admin). Licence je vázaná na IČO a lze ji používat na jednom zařízení (počítači). Pro využití SW nástroje na více počítačích je třeba si přikoupit další klientské licence.

V případě větší organizace je vhodná taktéž jedna administrátorská licence a volitelný počet klientských licencí ať už pro zaměstnance organizace nebo formou zprostředkovaných licencí pro třetí stranu (například obchodním partnerům). V případě udělení přístupu třetí straně je třeba vhodně definovat práva a povinnosti přímo v nástroji.

Další možností je multilicence, která je vhodná při využívání nástroje více firmami (od 1–255 firem/IČO). V tomto případě si každá firma zakoupí jednu klientskou licenci, která

je součástí multilicence. Každá licence je vázaná na jedno IČO dané firmy a pod každou takovou licencí může být neomezený počet klientů.

Dodavatel SW nástroje nabízí i customizované řešení variabilního licencování pro organizace s potřebou většího počtu licencí.

V ceně roční licence je bezplatná podpora a upgrade SW po dobu jednoho roku. Po uplynutí této lhůty (12 měsíců od instalace SW) lze využít obnovení tzv. maintenance (údržby a podpory SW) v ceně 10 % z pořizovací hodnoty SW (46).

3.6.3 Systémové požadavky

SW nástroj pracuje na principu tlustého klienta s databází MSSQL (Microsoft od verze 2014). Přičemž databáze může být umístěna na lokálním počítači, serveru s OS Windows nebo v cloudovém úložišti. Instalační soubor obsahuje všechny části systému spolu s databázovým serverem. Součástí každé licence je instalační manuál, uživatelská příručka, pravidelná aktualizace a garantovaný soulad s platnou legislativou. Software lze propojit se systémy SAP (51).

Minimální systémové požadavky na spuštění SW nástroje jsou:

- operační systém Windows 7 SP1 a vyšší,
- 2 GB RAM,
- NET Framework 4.5,
- Databázový server SQL nebo předplatné Windows Azure (balíček obsahuje Microsoft SQL server),
- 10 GB volného místa na systémovém disku,
- Rozlišení monitoru 1920x1080 (51).

3.6.4 Podporované bezpečnostní modely

Bezpečnostní model pro informační systém podle základních pravidel IB a osvědčených postupů.

Tento bezpečnostní model je vhodný pro řízení kybernetické bezpečnosti informačních systémů malých a středně velkých organizací, nezařazených mezi povinné subjekty mající uloženy povinnosti ve smyslu § 3 ZKB, ve znění pozdějších předpisů. Model

slouží jako nástroj řízení informační bezpečnosti a stanovení základních bezpečnostních opatření pro dosažení přiměřené odolnosti vůči kybernetickým hrozbám a útokům.

Bezpečnostní model pro informační systém podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.

Tento model slouží k řízení kybernetické bezpečnosti v rozsahu VKB ve znění pozdějších předpisů.

Kombinovaný bezpečnostní model pro informační systém podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. a podle základních pravidel IB.

Tento bezpečnostní model je vhodný pro řízení kybernetické bezpečnosti v kombinovaném rozsahu daném VKB ve znění pozdějších předpisů doplněnou o bezpečnostní opatření vycházejících ze základních pravidel IB a osvědčených postupů (best practice).

3.7 Odhad doby trvání implementace

Pro odhad doby trvání realizace implementace jsem využila metodu síťové analýzy s využitím programu Microsoft Project. K určení doby trvání jsem využila zkušenostních odhadů (tj. časové a termínové extrapolace z analogických projektů).

Tabulka jednotlivých činností v rámci implementace a síťový diagram jsou součástí **přílohy 2 a 3**. Kritická cesta (časově nejdelší možná cesta) v síťovém grafu je vyznačena červeně. Odhadovaná doba trvání celé realizace je 83 dní.

4 NÁVRHY ŘEŠENÍ

V návrhové části nejdříve stanovím postup a metodiku implementace. Podkapitoly jsou rozděleny podle jednotlivých kroků postupu skutečného průběhu implementace.

V době psaní diplomové práce nebyl vývoj nástroje kompletně dokončen. Při implementaci tedy uvádím i reálné připomínky, které byly vzneseny směrem k dodavateli nástroje.

4.1 Postup implementace softwarového nástroje ESKO

Při implementaci softwarového nástroje ESKO byl postup následovný:

1. Úvodní schůzka (kick-off meeting) se zadavatelem (určení požadavků zadavatele, stanovení odpovědností) *(částečně viz Analytická část)*
2. Odhad doby trvání implementace *(viz Analytická část)*
3. Druhá schůzka se zadavatelem, sběr podkladů
4. Analýza současného stavu společnosti *(viz Analytická část)*
5. Analýza a výběr nástroje *(viz Analytická část)*
6. Odsouhlasení výběru zadavatelem *(viz Analytická část)*
7. Vytvoření metodiky implementace
8. Nákup licence, instalace
9. Realizace v rámci softwarového nástroje
    - Zadání informací o organizaci
    - Identifikace primárních aktiv (ve spolupráci s garanty aktiv)
    - Vyplnění základních údajů o službě a primárních aktivech
    - Určení bezpečnostního modelu
    - Definování personálií (Personální bezpečnost)
    - Vyplnění základních údajů o třetích stranách (Řízení třetích stran)
    - Hodnocení primárních aktiv z pohledu důvěrnosti, integrity, dostupnosti (CIA)
    - Uzpůsobení seznamu podpůrných aktiv pro software a naplnění databáze podpůrnými aktivy (Řízení aktiv)
    - Analýza rizik

- Vytvoření prvotní verze dokumentace

10. Ověřování správnosti výstupní dokumentace dodavatelem služeb
11. Představení dokumentace výboru pro řízení kybernetické bezpečnosti a rozhodnutí o akceptaci rizik
12. Zapracování případných obsahových změn do dokumentace dodavatelem služeb
13. Zaškolení klíčových uživatelů v práci s nástrojem
14. Časové a ekonomické zhodnocení
15. Odsouhlasení výstupů zadavatelem
16. Předání kompletního díla včetně dokumentace

Během celého procesu byly prováděny průběžné zálohy databáze na server, který v rámci svých služeb poskytuje firma vyvíjející nástroj.

V následujících podkapitolách jsou rozepsány jednotlivé kroky implementace. Vynechány jsou ty kroky, které jsou součástí analytické části práce, konkrétně kroky č. 2, 4, 5, 6.

4.1.1 Schůzky se zadavatelem

Úvodní schůzka (*Kick-off Meeting*) v prostorách elektrárny proběhla za účelem rekognoskace prostředí elektrárny a seznámení se s požadavky zadavatele za účasti MKB, garantů primárních aktiv a zaměstnanců dodavatele řešení (implementace). V průběhu schůzky byly stanoveny také cíle a záměry včetně projednání časového plánu implementace.

Vzhledem k tomu, že při implementaci je nutná úzká spolupráce garantů aktiv a implementačního týmu, byl stanoven komunikační kanál (e-mail, Microsoft Teams) pro tuto součinnost. Součástí schůzky bylo také vyjasnění rolí a odpovědností v rámci implementace (viz následující podkapitola).

Zároveň bylo dohodnuto, že výstupy vygenerované softwarovým nástrojem budou předloženy výboru pro řízení kybernetické bezpečnosti ke schválení.

Výstupem **druhé schůzky** bylo upřesnění požadavků na data a informace potřebné pro analýzu. Tato schůzka proběhla formou řízeného rozhovoru s garantem primárních aktiv.

Požadavky zadavatele definované v této fázi jsou blíže specifikovány v kapitole 3.2 v *analytické části.*

4.1.2 Role v rámci implementace

Před započetím implementace je nutno vymezit role a odpovědnosti všech zúčastněných stran.

1 Role na straně zákazníka

Výbor kybernetické bezpečnosti:

- stanovuje bezpečnostní cíle,
- stanovuje požadavky pro výběr softwarového nástroje,
- schvaluje výsledné výstupy.

Manažer kybernetické bezpečnosti:

- zajišťuje součinnost s dodavatelem služeb,
- poskytuje dodavateli služeb potřebná data a informace,
- kontroluje a schvaluje průběžné výstupy ze SW nástroje a předkládá je výboru kybernetické bezpečnosti ke schválení.

Garanti aktiv:

- vystupují v roli klíčových uživatelů nástroje,
- poskytují dodavateli služeb potřebná data a informace,
- účastní se školení realizovaných dodavatelem,
- testují implementaci SW nástroje.

Vedoucí ekonomického oddělení:

- alokuje a schvaluje zdroje na implementaci.

2 Na straně dodavatele služeb

Manažer

- odpovědnost za dodávku služeb,
- zajišťuje součinnost se zákazníkem,
- kontroluje vytyčené cíle a plány,
- alokuje práci členů týmu a vede tento tým,

- odpovídá za plnění a provedení plánu ve stanoveném časovém a rozpočtovém rámci se snahou uspokojit zákazníka.

Technický konzultant

- odpovídá za kvalitu provedení implementace,
- podílí se na samotné implementaci,
- testuje softwarový nástroj a jeho implementaci,
- vznáší požadavky na změnu směrem k dodavateli nástroje,
- provádí školení pro oddělení IT zákazníka.

Konzultant kybernetické bezpečnosti

- ověřuje, zda je nástroj v souladu s požadavky VKB,
- podává zpětnou vazbu dodavateli nástroje.

3 Na straně dodavatele nástroje

Manažer a vlastník produktu:

- odpovědný za kvalitu produktu (SW nástroje),
- odpovědný za dodání produktu,
- zajišťuje součinnost s dodavatelem služeb,
- poskytuje lidské a další potřebné zdroje pro dodání SW nástroje,
- posuzuje, zda jsou změny na produktu proveditelné a/nebo přínosné.

Vývojář

- realizuje změnové požadavky SW nástroje,
- řeší problémy SW nástroje,
- testuje softwarové úpravy,
- posuzuje požadavky na změnu SW nástroje z technického hlediska.

Odborný garant kybernetické bezpečnosti

- odpovídá za úpravy v souladu s požadavky dodavatele služeb v oblasti kybernetické bezpečnosti,
- zajišťuje formální i obsahovou stránku výstupů generovaných nástrojem ESKO (analýza rizik, PoA atd.).

Helpdesk

- přijímá zákaznické požadavky,
- zajišťuje technickou podpora první a druhé úrovně.

4.1.3 Vytvoření metodiky implementace

V následujících kapitolách stanovím metodiku řízení aktiv a rizik v rámci implementace SW nástroje ESKO a souvisejících úkonů s následným uplatněním této metodiky přímo v nástroji.

Při tvorbě metodiky vycházím z VKB a ZKB s přihlédnutím k normám řady ISO/IEC 27000, zejména k ISO/IEC 27005, která je vhodnou pomůckou obsahující doporučení k identifikaci a hodnocení aktiv a řízení rizik bezpečnosti informací. K sestavení metodiky využívám i manuál poskytnutý firmou vyvíjející nástroj (49).

4.1.4 Nákup licence a instalace nástroje

V tabulce 4 jsou přehledně zaznačeny kroky, které bylo nutné provést pro úspěšnou instalaci nástroje.

Pro instalace softwaru ESKO byla zakoupena elektronická licence na webových stránkách dodavatele SW. Po zakoupení elektronické licence zákazník obdrží přihlašovací jméno a heslo pro aktivaci licence v SW nástroji. Instalační soubor si stáhne na webových stránkách.

Tabulka 4: Instalace nástroje ESKO (Zdroj: Vlastní zpracování)

Činnost	Postup	Problém	Doba trvání (člověkohodiny)
Zakoupení elektronické licence a získání přihlašovacích údajů pro aktivaci licence	Zakoupeno na webových stránkách po telefonické domluvě s dodavatelem SW nástroje		**1**
Stažení instalačního souboru softwaru	Staženo z odkazu uvedeného v návodu na instalaci		**2**
Nastavení uživatelských práv	Změna omezených oprávnění OS Windows na administrátorská práva		
Instalace ESKO software	Spuštění instalace, volby jazyka softwaru, odsouhlasení licenční smlouvy	Upozornění na chybějící .NET Framework 4.5	
Instalace .NET Framework 4.5	Staženo na oficiálních stránkách Microsoft		
Dokončení instalace ESKO SW	Opětovné spuštění a dokončení instalace		
Vypnutí antivirového programu	Pro korektní instalaci MSSQL serveru je třeba vypnout antivirový program		**3**
Instalace MSSQL Server	Spuštěna automaticky po instalaci ESKO SW, volba možnosti „New SQL stand-alone installation“, odsouhlasení licenčních podmínek	Chybová hláška „server s názvem MSSQLSERVER je již nainstalovaný"	
Vyřešení chybové hlášky	Přepis názvu v kolonce „Named instance“ na „MSQLSERVER_ESKO“		
Dokončení instalace MSSQL Server	Přidání uživatelů s administrátorským oprávněním k MSSQL serveru v kolonce „Specify SQL Server administrators“	Chybová hláška „NetFx3, Error Code: -2146498298“, která značí absenci .NET Framework 3.5	
Aktivace .NET Framework 3.5	Otevření – Ovládací panely\Všechny položky Ovládacích panelů\Programy a funkce – Zapnout nebo vypnout funkce systému Windows a označení možnosti – .NET Framework 3.5		
Restartování systému Windows a opakování instalace	Restartování OS a opětovné spuštění instalace		
Instalace dokončena	V instalačním okně se objeví potvrzení korektní instalace „Complete“		
Spuštění aplikace	Spuštění nainstalované aplikace	Aplikace vyžaduje instalaci „Microsoft Office Access database engine 2007“	**2**
Instalace „Microsoft Office Access database engine 2007“	Instalační okno se objeví automaticky při spuštění aplikace, odsouhlasení instalace		
Dokončení spuštění aplikace a aktivace licence	Výběr jazyka, Aktivace licence (zadání přihlašovacích údajů, volba „Aktivovat“)		
Výběr modulu	Volba modulu „Kybernetická bezpečnost organizace“		
Nastavení aplikace	Volba možnosti „Vytvořit připojení k databázi“; změna názvu serveru na „MSQLSERVER_ESKO“; volba možnosti „Otestovat připojení“; po zobrazení okna „Chcete vytvořit databázi?“ volba možnosti „Ano“; úspěšné vytvoření databáze		
Restartování aplikace a doplňující nastavení	Automatické restartování a opětovné spuštění nastavení; volba možnosti „Zadat nového správce“ (Zadání údajů o správci s oprávněním admin, uživatelského jména a hesla), volba „Přejít do aplikace“		
Celkem			**8**

Instalace nástroje ESKO včetně instalace serveru MSSQL (růžové řádky v tabulce) a řešení chybových hlášení trvala 8 člověkohodin.

4.1.5 Realizace v rámci softwarového nástroje

V následujících podkapitolách jsou popsány jednotlivé kroky stanovené metodiky implementace (*metodika*), ke které vzápětí uvádím její uplatnění v nástroji ESKO (*ESKO implementace*).

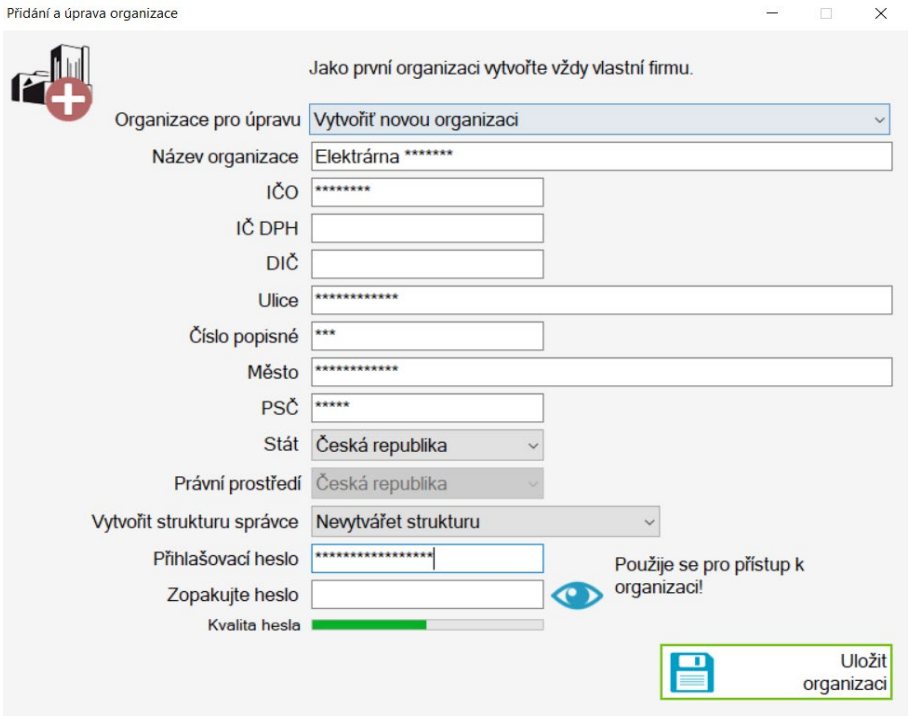
I. Zadání informací o organizaci

Metodika: Základní údaje o organizaci, které byly nashromážděny v analytické části práce, se zaznamenají do příslušných záložek (karet) v prostředí SW nástroje ESKO.

ESKO implementace: Organizaci založím v záložce „Organizace – Přidání a úprava“, kde vyplním základní údaje včetně příslušného legislativního rámce. Vybírám právní prostředí „Česká republika“ (nástroj je přizpůsoben rovněž pro právní prostředí Slovenské republiky).

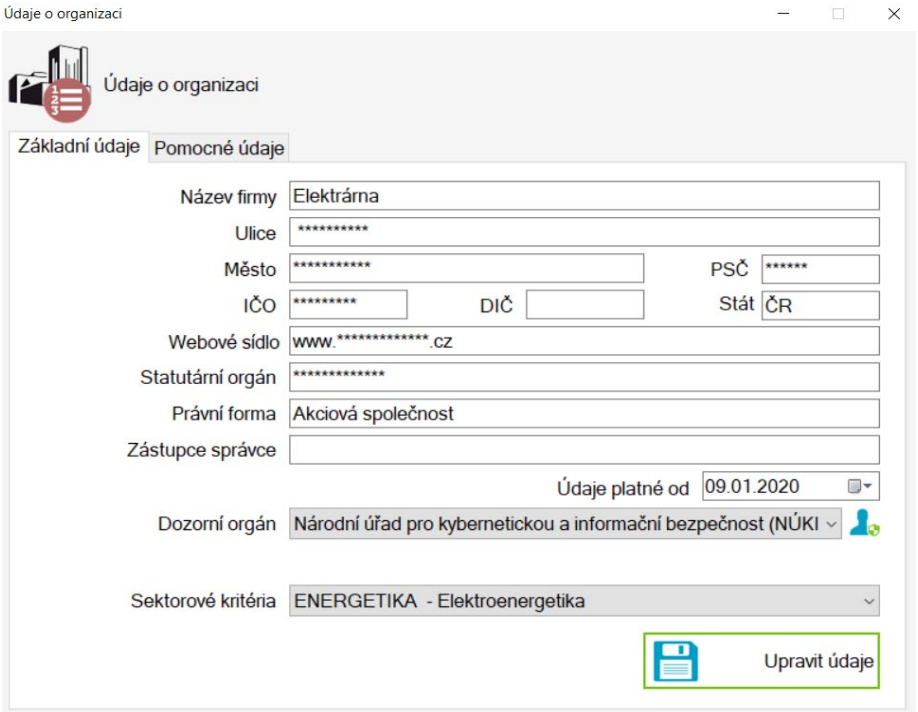
Po založení organizace zadám doplňující údaje o organizaci jako je právní forma a zadám dozorový orgán, kterým je v tomto případě Národní úřad pro kybernetickou a informační bezpečnost. Od volby sektorových kritérií „Energetika – elektroenergetika“ se budou odvíjet data v číselnících.

Uplatnění popsaného postupu v nástroji ESKO je vidět na obrázku 14 a 15.



Obrázek 14: Přidání a úprava organizace (Zdroj: Nástroj ESKO)

Na obrázku 15 je vidět karta se základními údaji o organizaci.



Obrázek 15: Údaje o organizaci (Zdroj: Nástroj ESKO)

Primární a podpůrná aktiva

Před samotným naplněním nástroje aktivy je třeba provést identifikaci a hodnocení primárních a podpůrných aktiv, jedná se o podmínku pro splnění požadavků kybernetického zákona.

V nástroji ESKO slouží tato identifikace k následnému řízení kybernetické bezpečnosti včetně řízení procesů, aktiv, rizik, personální bezpečnosti a evidování třetích stran položka základního výběru „Bezpečnost IKT".

RASCI matice

Metodika: Prvním krokem ve fázi identifikace a hodnocení aktiv je definování odpovědností. Pomocí RASCI matice odpovědnosti přiřadím jednotlivým činnostem role a jejich odpovědnosti na straně analyzované společnosti.

ESKO implementace: RASCI matici vytvořím pomocí programu v záložce „Audity – RASCI". Výstup vidíme v tabulce 5. RASCI matice vychází z normy ČSN ISO/IEC 27002, konkrétně kapitoly „Řízení aktiv" (24) .

Odpovědnosti jsou v RASCI matici označeny písmeny, jejichž význam je následující:

- **R** *Responsible* – odpovědnost (odpovědnost za vyhotovení dílčí činnosti)
- **A** *Accountable* – vrcholová odpovědnost (odpovědnost za schvalování hotového úkolu)
- **S** *Supportive* – podíl/podpora při činnosti (odpovědnost za poskytování dalších zdrojů potřebných k realizaci činnosti, podpůrná role při implementaci)
- **C** *Consulted* – podíl na činnosti (role, která má informace nebo znalosti k pokroku/ukončení činnosti, oboustranná komunikace)
- **I** *Informed* – informovanost o průběhu a výsledcích činnosti (role má být informována o pokroku a výsledcích, jednostranná komunikace) (52).

Tabulka 5: RASCI matice (Zdroj: Vlastní zpracování pomocí softwaru ESKO)

R = Responsible A = Accountable S = Supportive C = Consulted I = Informed			role													
			garant aktiva	zaměstnanec (uživatel)	vrcholové vedení	ředitel odd.	výbor pro řízení KB	manažer KB	IT bezpečnostní odd.	HR	veřejné zakázky	právní oddělení	ekonomické oddělení	oddělení provozní	CIO / IT ředitel
činnosti podle normy ČSN ISO/IEC 27002																
Název		**Opatření**														
A.8.1.1	Seznam aktiv organizace	*Aktiva související s informacemi a prostředky pro zpracování informací musí být identifikována a seznam těchto aktiv musí být vytvořen a udržován aktuální.*	**A**				**S**	**R**			**R**				**C**
A.8.1.2	Vlastnictví aktiv	*Aktiva udržovaná v seznamu musí mít určeného vlastníka.*	**A**			**R**	**S**	**R**					**S**	**S**	**C**
A.8.1.3	Přípustné použití aktiv	*Musí být určena, dokumentována a implementována pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a prostředky pro zpracování informací.*	**A**	**I**			**R**	**S**	**C**	**S**	**C**			**S**	
A.8.1.4	Navrácení aktiv organizace	*Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci a pracovníci externích stran odevzdat veškerá jim svěřená aktiva, která jsou majetkem organizace.*	**A**	**I**		**R**	**C**			**S**	**S**		**C**	**S**	**S**
A.8.2.1	Klasifikace informací	*Informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci.*	**A**	**I**		**S**	**R**	**C**							
A.8.2.2	Označování informací	*Pro označování informací musí být vytvořeny a implementovány postupy, které jsou v souladu se schématem klasifikace informací přijatým organizací.*	**A**	**I**			**S**	**R**		**C**	**C**	**C**	**C**	**S**	**S**
A.8.2.3	Manipulace s aktivy	*Pro manipulaci s aktivy musí být vytvořeny a implementovány postupy v souladu se schématem klasifikace informací přijatým organizací.*	**A**	**I**			**C**	**S**					**C**	**S**	**R**
A.8.3.1	Správa výměnných médií	*Musí být implementovány postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatým organizací.*	**A**	**I**			**S**	**S**	**C**					**S**	**R**
A.8.3.2	Likvidace médií	*Média, pokud nejsou dále upotřebitelná, musí být bezpečně zlikvidována v souladu s formalizovanými postupy.*	**A**	**I**			**S**						**C**		**R**
A.8.3.3	Přeprava fyzických médií	*Média obsahující informace musí být během přepravy chráněna proti neoprávněnému přístupu, zneužití nebo narušení.*	**A**	**I**			**S**	**C**	**C**						**R**

II. Identifikace primárních aktiv

Metodika: Důležitým krokem identifikace a hodnocení aktiv je správné vymezení hranice prvků kritické infrastruktury. Jedná se o určení, která aktiva jsou součástí KII a na která už se naopak ZKB nevztahuje. Identifikaci i hodnocení by měla provádět kompetentní osoba nebo kolektiv kompetentních osob s dobrou znalostí daných procesů, respektive aktiv, tedy nejčastěji vlastníci (garanti) aktiv, jako jsou IT pracovníci, klíčoví uživatelé atd.

Následující doporučení vychází z doporučení normy ISO/EIC 27005 pro identifikaci primárních aktiv.

Doporučuje se identifikovat procesy a činnosti:

- jejichž ztráta nebo omezení neumožňuje plnit poslání společnosti, jakožto výrobce elektřiny a poskytovatele podpůrných služeb,
- jejichž pozměnění může významně ovlivnit plnění poslání společnosti, jakožto výrobce elektřiny a poskytovatele podpůrných služeb,
- jejichž fungování je nutné pro plnění smluvních, právních nebo regulačních požadavků,
- obsahující utajené skutečnosti, patentované či chráněné technologie (23).

Doporučuje se identifikovat zejména citlivé informace:

- životně důležité pro plnění činnosti společnosti, jakožto výrobce elektřiny a poskytovatele podpůrných služeb,
- osobní údaje, ve smyslu zákona o ochraně osobních údajů,
- strategické a utajované informace, vyžadované pro dosažení strategických cílů společnosti, jejichž shromažďování, skladování, zpracování a přenos jsou časově nebo finančně náročné (23).

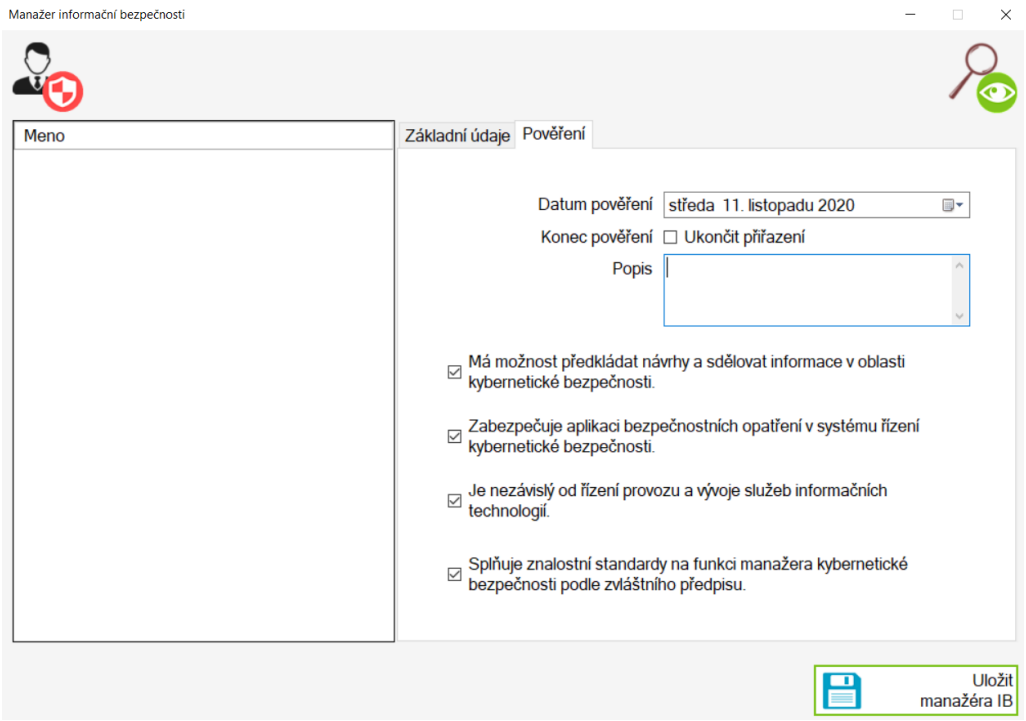
Dalším krokem je sestavení seznamu garantů primárních aktiv.

ESKO implementace: Jako primární aktivum byla stanovena následující služba se zohledněním kritérii KII:

- výroba elektřiny a poskytování podpůrných služeb,

Nejdříve zaeviduji identifikační a kontaktní údaje o MKB v záložce „Bezpečnost IKT – Manažer informační bezpečnosti“. V kartě „Základní údaje“ zaznamenávám informace

jako titul, jméno, příjmení, adresa, e-mail, telefon. V kartě „Pověření“ se upřesňuje pověření MKB, jak lze vidět na obrázku 16.



Obrázek 16: Manažer informační bezpečnosti – Pověření (Zdroj: Nástroj ESKO)

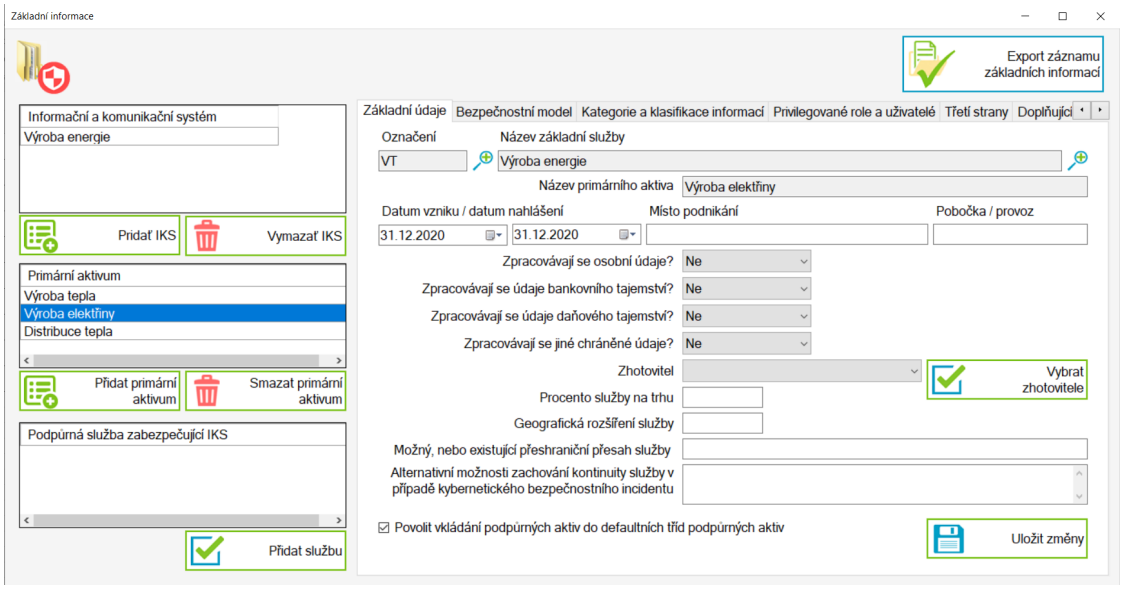
Rozpor s ZKB: „Manažer informační bezpečnosti“ je v terminologickém rozporu s VKB. Termín by měl být nahrazen za „Manažer kybernetické bezpečnosti“.

III. Vyplnění základních údajů o službě a primárních aktivech

ESKO implementace: V záložce „Bezpečnost IKT – Základní informace“ nejdřív přidáváme informační a komunikační systém. V případě elektrárny nelze určit nadřazený IS, proto zde uvádím nadřazenou službu „Výroba energie“ (tlačítko Přidat IKS). Následně přidám primární aktiva (Přidat primární aktivum) a specifikuji parametry v záložce „Základní údaje“ (název, datum vzniku /datum nahlášení služby, místo podnikání, pobočka /provoz, údaj, zda se zpracovávají osobní údaje, údaje bankovního tajemství, údaje daňového tajemství, údaj o zhotoviteli a další doplňující údaje).

Pro účely této implementace zaškrtnu možnost „Povolit vkládání podpůrných aktiv do defaultních tříd podpůrných aktiv”. Tuto možnost volím, protože má elektrárna specifická podpůrná aktiva a nelze tedy využít pouze přednastavených tříd aktiv. Třídy aktiv, které defaultně neobsahují žádná podpůrná aktiva, budou v dalších krocích dále

detailizovány. Vzhledem k tomu, že zde identifikuji proces nikoli IS, *zhotovitele* nezadávám. Na obrázku 17 je vidět karta „Základní informace“.



Obrázek 17: Základní informace (Zdroj: Nástroj ESKO)

Rozpor s ZKB: U této záložky je terminologický rozpor s ZKB. V „Základních údajích“ se definuje „Název základní služby“. Dle ZKB se řadí do základní služby pouze služby nebo IS uvedené v kapitole 2.14. Zvolený název však nelze použít obecně na všechny subjekty, kterým je software nabízen.

IV. Určení bezpečnostního modelu

Metodika: Bezpečnostní model je určen stanoveným rozsahem, který určuje VKB.

ESKO implementace: V záložce „Bezpečnostní model“ jsem v závislosti na stanoveném rozsahu (viz kapitola 3.4) vybrala model „Bezpečnostní model pro informační systém podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.“ (popis bezpečnostních modulů viz kapitola 3.6.4).

V. Definování personálií

Metodika: K identifikovaným aktivům je třeba přiřadit garanta. Garant každého aktiva je stanoven manažerem kybernetické bezpečnosti (MKB) ve spolupráci s výborem kybernetické bezpečnosti.

Garantem aktiva je nejčastěji stanoven pracovník, respektive pracovníci organizačního útvaru, jehož pracovní náplň souvisí s regulovaným systémem, popřípadě pracovník útvaru, kde dochází ke zpracování primárních aktiv.

MKB obeznámí garanty s požadavky ZKB a dále pracují v součinnosti. MKB tyto garanty aktiv eviduje.

Stanovení a zaevidovaní garanti mají za úkol upřesnit parametry primárních aktiv. MKB garanty obeznámí s metodou hodnocení aktiv z hlediska důvěrnosti, dostupnosti a integrity (CIA).

ESKO implementace: Předtím než přiřadíme primárním aktivům jejich garanty, je třeba si v záložce „Bezpečnost IKT – Personální bezpečnost" zaevidovat ty zaměstnance firmy, kterým budou následně přiřazeny role. Zaměstnance lze přidat přes možnost „Upravit zaměstnance – Přidat nového zaměstnance", kde zadávám nezbytné osobní a kontaktní údaje. Funkci zaměstnanci přiřadím tlačítkem „Upravit funkce" a pracoviště přes „Upravit pracoviště".

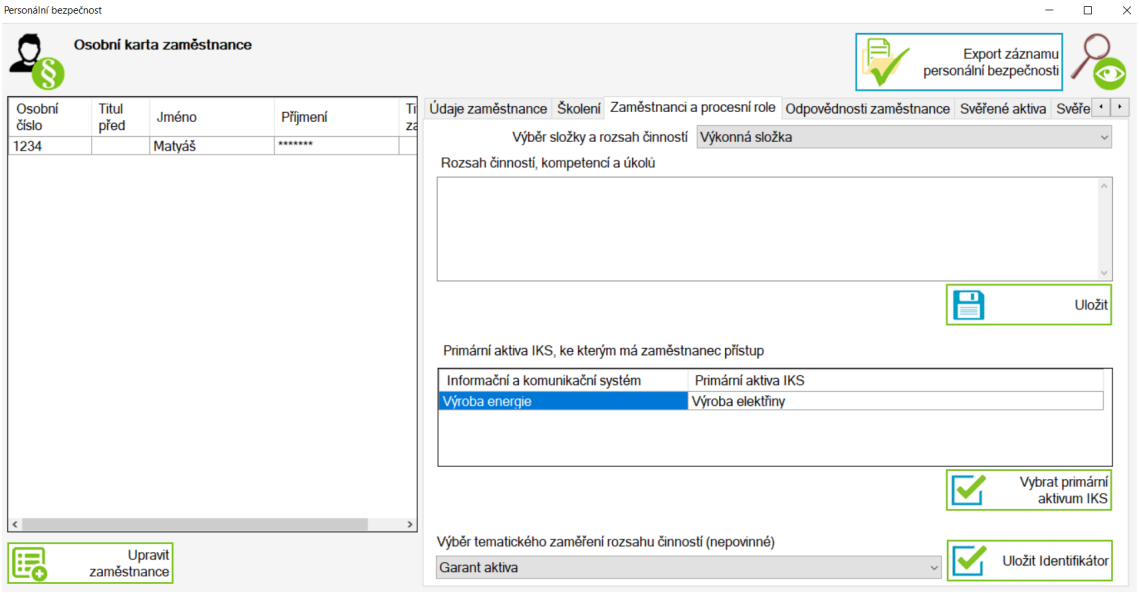
V záložce „Základní informace – Privilegované role a uživatelé" přiřazuji vybranému primárnímu aktivu zaměstnance spolu s jejich privilegovanými rolemi (Upravit seznam – Vybrat osobu). Určitému aktivu lze přiřadit více než jednoho zaměstnance a následně jim přiřadit různé role (např. administrátor, povolení vidět neveřejné aktivity atd.).

V kartě zaměstnance lze dále evidovat i údaje o školeních, rozsah činností, seznam odpovědností, údaj o delegování práv a povinností na jinou osobu, provedené kontroly a hodnocení. Tyto informace nebyly dodavateli poskytnuty a zadavatel si je bude vyplňovat postupně sám. Evidenci svěřených aktiv lze následně využít k inventarizaci.

Identifikace garanta primárního aktiva

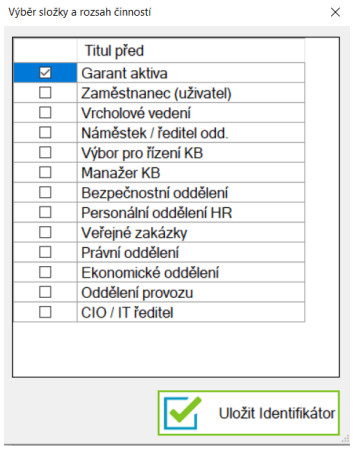
ESKO implementace: V záložce „Zaměstnanci a procesní role" určím zvolenému zaměstnanci „Výkonnou složku". Následně vyberu primární aktivum (Vybrat primární aktivum), ke kterému má zaměstnanec přístup. Vyberu tedy „výroba elektřiny" a přes tlačítko „Uložit identifikátor" vyberu procesní roli garanta aktiva.

Na obrázku 18 je zobrazena karta „Personální bezpečnost (Osobní karta zaměstnance)".



Obrázek 18: Přiřazení garanta k primárnímu aktivu (Zdroj: Nástroj ESKO)

Na obrázku 19 je výběr rolí, které lze zaměstnanci přiřadit.



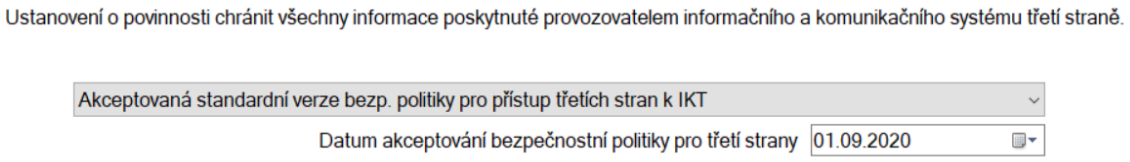
Obrázek 19: Procesní role (Zdroj: Nástroj ESKO)

VI. Vyplnění základních údajů o třetích stranách (Řízení třetích stran)

Metodika: Pro účely analýzy rizik jsou důležití pouze ti dodavatelé, jejichž služby jsou nezbytné pro zajištění správné a spolehlivé činnosti kritické informační infrastruktury (KII) elektrárny.

ESKO implementace: Třetí strany se evidují v záložce „Bezpečnost IKT – Řízení třetích stran", kde se vyplní základní údaje o třetích stranách. Přidám zde dodavatele definované v kapitole 3.1.3. Dodavateli lze časově vymezit oprávnění. Karta řízení třetích stran obsahuje také informace, ke kterým aktivům má dodavatel přístup a data uzavření,

respektive ukončení smlouvy. Následně je v záložce „Dodržování bezpečnostní politiky" uveden závazek třetí strany dodržovat bezpečnostní politiky a povinnosti, chránit všechny informace jí poskytnuté a závazek dodržovat a přijímat bezpečnostní opatření. Stanovené politiky lze pro přehlednost vložit (Vložit dokumenty).



Obrázek 20: Akceptace bezpečnostních politik dodavateli (Zdroj: Nástroj ESKO)

V kartě „Doplňující údaje" vložím smlouvy s dodavateli.

VII. Hodnocení primárních aktiv dle CIA

Metodika: Dále je třeba ohodnotit důležitost aktiv, která patří do stanoveného rozsahu, podle § 4 (Řízení aktiv) v rozsahu přílohy č. 1 vyhlášky č. 316/2014 Sb.

VKB stanovuje základní požadavky při hodnocení důležitosti primárních aktiv.

Je třeba posoudit alespoň:

- rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,
- rozsah dotčených právních povinností nebo jiných závazků,
- rozsah narušení vnitřních řídících a kontrolních činností,
- poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
- dopady na poskytování důležitých služeb,
- rozsah narušení běžných činností,
- dopady na zachování dobrého jména nebo ochranu dobré pověsti,
- dopady na bezpečnost a zdraví osob,
- dopady na mezinárodní vztahy,
- dopady na uživatele informačního a komunikačního systému (5).

Garant aktiva při svém hodnocení vychází z výše zmíněných aspektů. Hodnotí se především provozní informační systémy, procesy, informace a s nimi spojená aktiva.

Nejdříve uvedu metodiku hodnocení důležitosti primárních aktiv dle triády CIA.

Primární aktiva se hodnotí pomocí dopadové tabulky pro jednotlivé aspekty CIA. Celková hodnota důležitosti aktiva se rovná maximální hodnotě CIA. Je-li tedy aktivum ohodnoceno z hlediska důvěrnosti a integrity úrovní „nízká", avšak z hlediska dostupnosti úrovní „vysoká", zvolíme maximální hodnotu. Celková hodnota aktiva bude „vysoká".

Do hodnocení se zahrnují i aktiva, na kterých jsou závislá jiná aktiva a/nebo důležité obchodní procesy. Například v případě elektrárny závisí zachování klíčového obchodního procesu dodávky elektrické energie do energetické rozvodné sítě na správné funkci softwarového řídicího systému typu SCADA. Tyto netriviální závislosti se promítají do hodnoty posuzovaného aktiva. Pokud je hodnota posuzovaného aktiva (např. SCADA) větší nebo stejná jako hodnota aktiva, které na něm závisí (zde proces dodávky elektrické energie), zůstane hodnota posuzovaného aktiva stejná. Naopak pokud je hodnota posuzovaného aktiva (zde SCADA) menší než hodnota aktiva, které na něm závisí (zde proces dodávky elektrické energie do rozvodné sítě), pak se hodnota posuzovaného aktiva (SCADA) zvýší s přihlédnutím ke stupni závislosti až na hodnotu aktiva nebo důležitého obchodního procesu (dodávka energie), které na něm závisí. Při zvyšování hodnoty posuzovaného aktiva na základě závislostí se přihlíží ke stupni závislosti a k hodnotám ostatních závislých aktiv (v případě více než jedné závislosti) (23).

Skutečnost, že posuzovaná elektrárna je začleněna do kritické infrastruktury státu, ovlivňuje hodnocení dle CIA. Klíčovým kritériem je zachování schopnosti společnosti vyrábět elektřinu a poskytovat podpůrné služby.

Hlavní kritéria, která budou zohledněna při posuzování možných následků ztráty důvěrnosti, integrity a dostupnosti jsou následující:

- přerušení výroby elektřiny,
- neschopnost poskytovat podpůrné služby,
- ohrožení bezpečnosti nebo zdraví odběratelů, zaměstnanců nebo pracovníků dodavatelů,
- ohrožení bezpečnosti životního prostředí,
- ohrožení integrity nebo životnosti technologického celku,
- porušení právních předpisů nebo smluvních závazků,
- porušení povinnosti stanovené regulátorem trhu,
- vznik významné finanční ztráty nebo škody na majetku,
- ztráta zákazníků,

- únik citlivých osobních údajů (23).

Hodnocení dle CIA je subjektivně závislé na hodnotiteli. V zájmu udržení maximální možné objektivity je doporučeno se v rámci tohoto hodnocení držet následujících zásad:

- transparentnost a přezkoumatelnost – vždy uvádět důvody které vedly ke stanovení příslušné úrovně hodnocení aktiv,
- předběžná opatrnost – je-li aktivum hodnoceno více hodnotiteli, nebo je-li aktivum hodnoceno s použitím různých přístupů (např. z hlediska nákladů, z hlediska dopadů při incidentu apod.), je jako výsledná hodnota stanovena nejvyšší dosažená úroveň hodnocení,
- objektivnost – aktiva by měla být hodnocena garantem aktiva i MKB.

Výstupem hodnocení je seznam ohodnocených aktiv (klíčových prvků systémů), kde u jednotlivých aktiv je uvedena dosažená celková důležitost aktiva. Z tohoto seznamu aktiv bude vycházet následná analýza rizik.

Stupnice pro hodnocení převzaté z VKB jsou zaznamenány v tabulce 6, 7, 8.

Tabulka 6: Stupnice pro hodnocení důvěrnosti (C) (Zdroj: (5))

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická.

Tabulka 7: Stupnice pro hodnocení integrity (I) (Zdroj: (5))

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

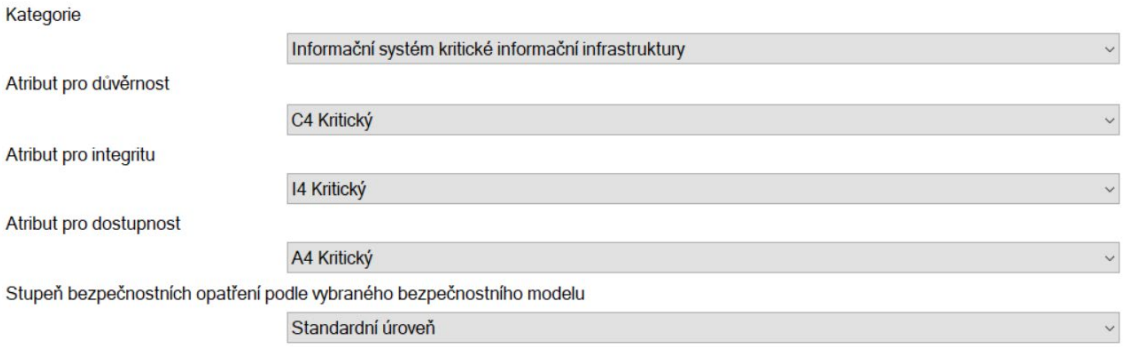
Tabulka 8: Stupnice pro hodnocení dostupnosti (A) (Zdroj: (5))

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

ESKO implementace: V záložce „Základní informace – Kategorie a klasifikace informací“ volím kategorii služby „Výroba energie” jako „Informační systém kritické infrastruktury“. Následně ohodnotím proces definovaný jako primární aktivum „Výroba

elektřiny" z hlediska atributů CIA. U stupně bezpečnostního opatření volím standardní úroveň. V závislosti na zvolené úrovni budou generována opatření v analýze rizik.

Klasifikaci vidíme na obrázku 21.



Obrázek 21: Hodnocení aktiv dle triády CIA (Zdroj: Nástroj ESKO)

VIII. Naplnění databáze podpůrnými aktivy (Řízení aktiv)

Seznam podpůrných aktiv včetně jejich ohodnocení, poskytnutý MKB, se musel uzpůsobit pro potřeby nástroje. Nástroj zavádí kategorizaci podpůrných aktiv do takzvaných *tříd aktiv*, což je seskupení dílčích podpůrných aktiv stejné povahy a typu. Uzpůsobený seznam s rozřazením podpůrných aktiv do těchto tříd je v **příloze 4 a 5**.

Identifikace podpůrných aktiv

Metodika: Při identifikaci podpůrných aktiv MKB zjišťuje od garantů primárních aktiv, jaká aktiva jsou závislá na primárních aktivech. Vzhledem k tomu, že systém podpůrných aktiv bývá velmi rozsáhlý, je vhodnější je nejdříve posuzovat na úrovni funkčního celku (např. podle lokality, procesu atd.) a až poté na detailnější úrovni samotných komponent funkčních celků.

ESKO implementace: V nástroji ESKO jsem aktiva rozřadila do funkčních celků podle předdefinovaných *tříd aktiv*.

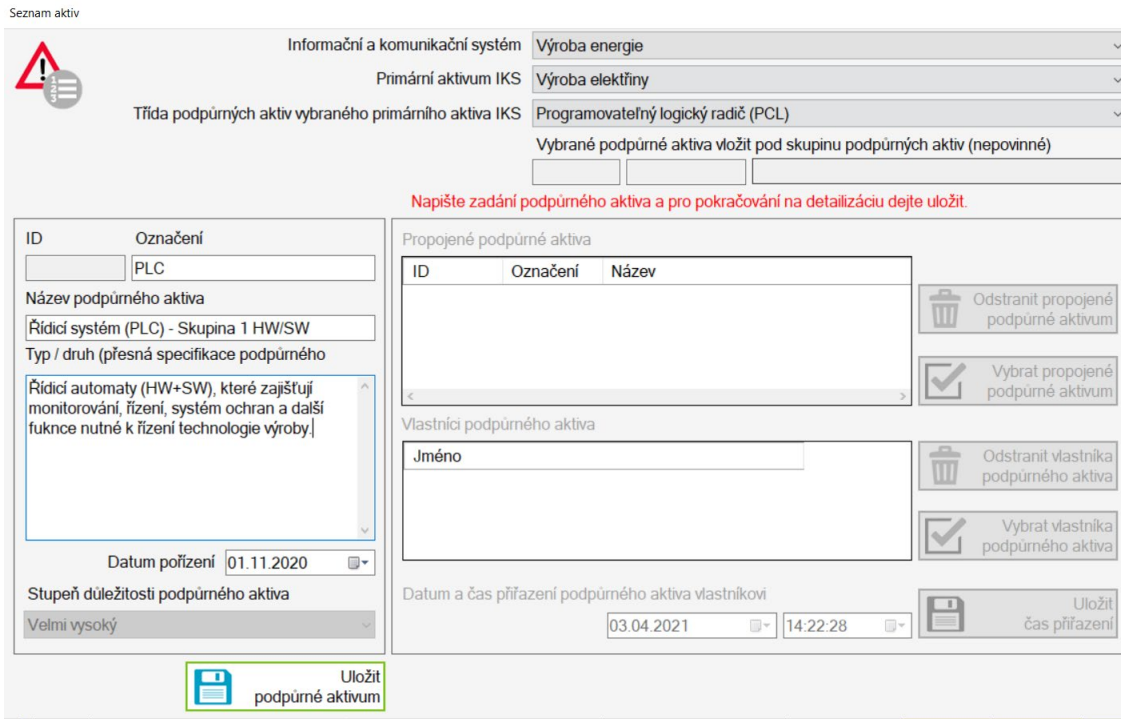
Vazby mezi aktivy

Metodika: MKB spolu s garanty primárních a podpůrných aktiv stanoví vazby (závislosti) mezi primárními a podpůrnými aktivy a následně zhodnotí důsledky těchto vazeb. Hodnocení podpůrných aktiv se dědí z hodnoty závislých primárních aktiv, popřípadě závislých nadřazených podpůrných aktiv.

ESKO implementace: Dělení aktiv do tříd se využívá při následné analýze rizik a umožňuje posuzovat rizika většího počtu aktiv se stejnou úrovní bezpečnosti.

Nová podpůrná aktiva se přidávají přes záložku „Seznam podpůrných aktiv". Zde postupně přidávám všechna podpůrná aktiva s upřesněním hlavních údajů jako označení aktiva, název aktiva, typ aktiva, datum zaevidování a stupeň důležitosti. Tímto způsobem rozšiřují „číselník podpůrných aktiv" o aktiva, která nejsou zařazena v defaultním seznamu aktiv. V záložce taky volím primární aktivum, na kterém je podpůrné aktivum závislé spolu se službou a třídou podpůrných aktiv, ke kterým má být podpůrné aktivum přiřazeno.

Na obrázku 22 je vidět přidání nového podpůrného aktiva *PLC*, které je zařazeno do třídy aktiv *Programovatelný logický řadič*.



Obrázek 22: Seznam aktiv (Zdroj: Nástroj ESKO)

Identifikace garantů podpůrných aktiv

Metodika: Po identifikaci podpůrných aktiv MKB následně zjistí, popřípadě určí a zaeviduje garanty podpůrných aktiv. Garanti podpůrných aktiv upřesní s pomocí MKB parametry podpůrných aktiv.

ESKO implementace: Po uložení se zpřístupní další části okna, kde je možnost vybrat vlastníka (garanta) podpůrného aktiva s uvedením data a času přiřazení a další propojená (závislá) podpůrná aktiva.

Po přidání všech podpůrných aktiv doplním další jejich nezbytné parametry v záložce „Řízení aktiv". Do analýzy vstupují samotné třídy podpůrných aktiv, jako seskupení jednotlivých podpůrných aktiv shodného druhu a se stejnou rizikovostí (pokud nezvolíme jinak), resp. se shodnými hrozbami a zranitelnostmi.

V kartě „Řízení aktiv" lze doplnit následující:

- popis třídy podpůrných aktiv/podpůrného aktiva,
- detailizace třídy podpůrných aktiv/podpůrného aktiva včetně propojení s jinými aktivy,
- evidence vlastníků třídy podpůrných aktiv/podpůrného aktiva včetně možnosti přiřazení dokumentů v elektronické podobě, kterými byla třída/aktivum vlastníkem převzato,
- personálie třídy podpůrných aktiv/podpůrného aktiva včetně přiřazení odpovědné osoby za evidenci aktiva, osoby odpovědné za realizaci bezpečnostních opatření (BO) a správce třídy podpůrného aktiva,
- stupeň důležitosti třídy podpůrných aktiv/podpůrného aktiva,
- umístění třídy podpůrných aktiv/podpůrného aktiva.

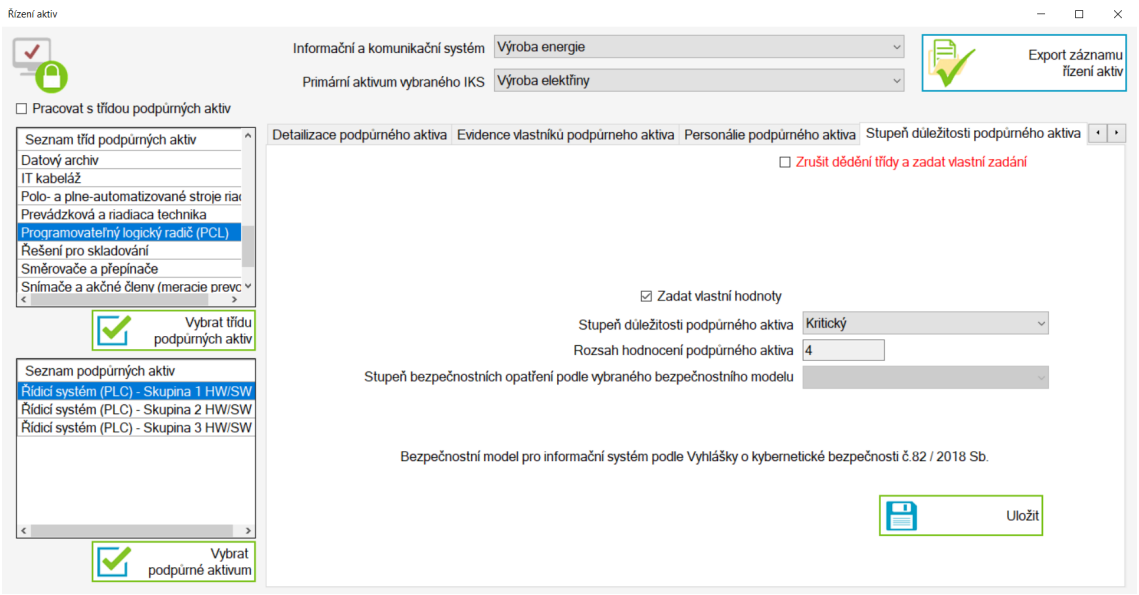
Jednotlivé parametry lze uvádět, jak pro třídy aktiv, tak pro jednotlivá dílčí aktiva zvlášť.

V kartě jsem přiřadila jednotlivým třídám aktiv jejich garanty (vlastníky). Následně jsem provedla detailizaci personálií. U všech evidovaných podpůrných aktiv je garant aktiv, odpovědná osoba za evidenci a realizaci bezpečnostních opatření a správce podpůrných aktiv.

Hodnocení podpůrných aktiv

Metodika: Na základě hodnocení podpůrných aktiv garanty těchto aktiv se stanoví celková důležitost podpůrných aktiv, respektive třídy podpůrných aktiv.

ESKO implementace: Dále je třeba stanovit celkovou úroveň důležitosti jednotlivých tříd podpůrných aktiv v záložce „Stupeň důležitosti třídy podpůrných aktiv“ (obrázek 23). Popřípadě lze po zrušení volby možnosti „pracovat s třídou podpůrných aktiv“ a „zrušit dědění třídy a zadat vlastní zadání“ ohodnotit každé podpůrné aktivum zvlášť.



Obrázek 23: Řízení aktiv (Zdroj: Nástroj ESKO)

Na obrázku 24 jsou stupně ohodnocení důležitosti (třídy) podpůrného aktiva v nástroji. Lze vybírat ze čtyř stupňů důležitosti.

Nízky	1
Střední	2
Vysoký	3
Kritický	4

Obrázek 24: Stupně hodnocení důležitosti (třídy) podpůrného aktiva (Zdroj: Nástroj ESKO)

Z karty „Řízení aktiv“ lze v případě potřeby vygenerovat záznam přes tlačítko „Export záznamu řízení aktiv“.

Manipulace, likvidace a zabezpečení aktiv

Metodika: Po zhodnocení primárních a podpůrných aktiv se stanoví a zavedou pravidla zabezpečení jednotlivých úrovní těchto aktiv. S ohledem na úroveň aktiv je třeba stanovit

přípustné způsoby jejich užívání a určit pravidla pro manipulaci s aktivy, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv.

Dále se určí způsob likvidace dat, provozních údajů, informací včetně jejich kopií. Určuje se i likvidace technických nosičů dat s ohledem na úroveň aktiv v souladu s přílohou č. 4 VKB (5).

ESKO implementace: V ESKO je likvidace aktiv součástí bezpečnostních opatření, kde se určují i osoby odpovědné za likvidaci.

IX. Analýza rizik

Součástí nástroje je registr (databáze) hrozeb a zranitelností vycházející z VKB a „best practice", které jsou namapovány na seznam ohodnocených aktiv.

Analýzu rizik je třeba provádět opakovaně a rizika revidovat. Pro systémy KII se hodnocení rizik musí dle VKB provádět alespoň jednou ročně a při významných změnách (5).

Volba rozsahu identifikace rizik

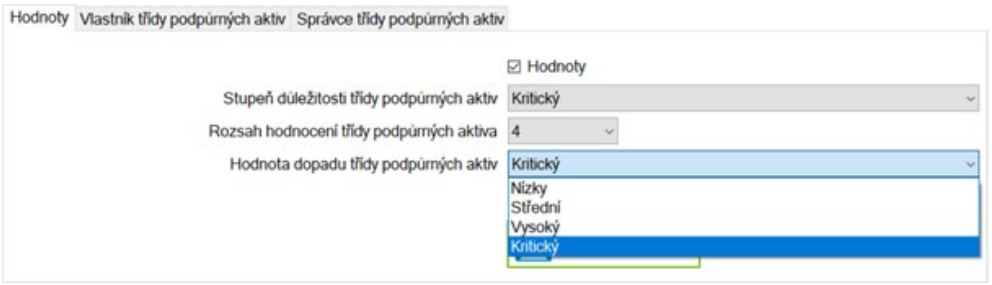
Metodika: Analýza rizik je prováděna u všech aktiv zahrnutých do stanoveného rozsahu. Vstupem pro polo-automatizovanou analýzu rizik v ESKO je ohodnocený seznam aktiv vyhotovený v předchozích krocích.

ESKO implementace: Poté co je databáze naplněna primárními a podpůrnými aktivy s příslušnými parametry a specifiky přecházím k samotné analýze rizik. Garanti jednotlivých aktiv byli formou školení seznámeni s metodikou pro řízení rizik.

Po kliknutí na záložku „Analýza rizik" vybírám možnost „Vytvořit novou AR", z nabízených možností volím „Vytvořit vstupní analýzu rizik" pro primární aktivum *výroba elektřiny* (stanovení rozsahu) a doplním název analýzy. V nabídce je dále možné vytvořit testovací analýzu rizik a průběžnou analýzu rizik, která bude využita klíčovými uživateli po implementaci nástroje.

Po přidání nové analýzy rizik se otevře okno analýzy rizik, kde je vidět přehled zvoleného bezpečnostního modelu, provedené hodnocení primárního aktiva dle CIA („Volba rozsahu identifikace rizik") a doplňující popis jednotlivých podpůrných aktiv a jejich garanti, popř. správci („Popis třídy podpůrných aktiv").

V případě potřeby lze změnit dříve zadané hodnocení důležitosti třídy podpůrných aktiv a nově zvolit hodnotu dopadu opět podle čtyřstupňové stupnice (nízký, střední, vysoký, kritický). Hodnota dopadu se automaticky načte na základě předešlého hodnocení důležitosti třídy podpůrného aktiva, popřípadě lze hodnotu změnit podle potřeb.

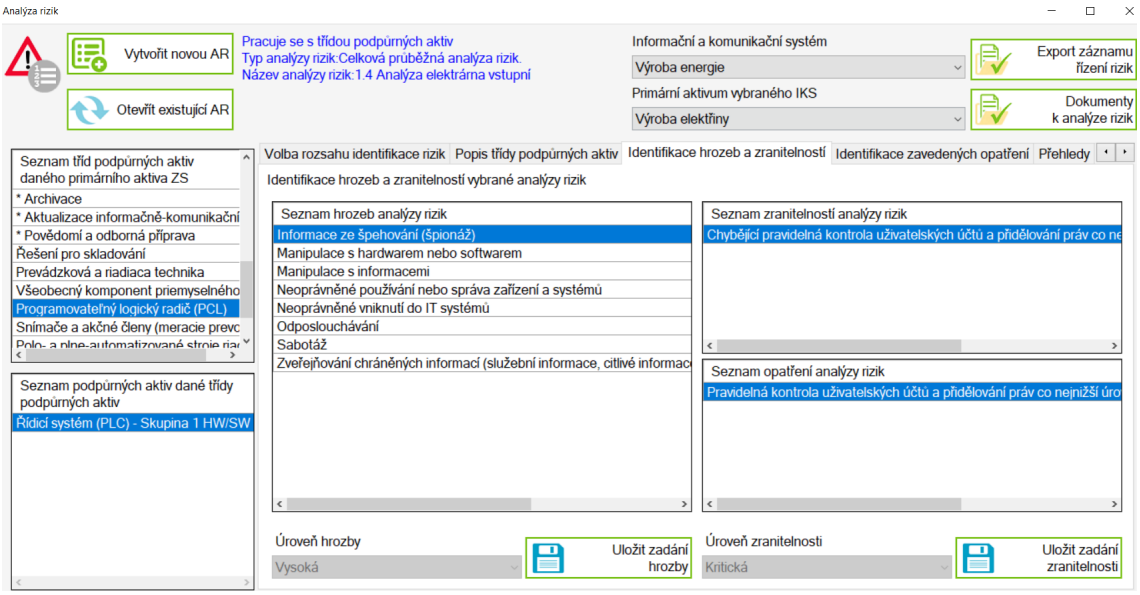


Obrázek 25: Hodnota dopadu třídy podpůrných aktiv (Zdroj: Nástroj ESKO)

Identifikace hrozeb, zranitelností a zavedených opatření

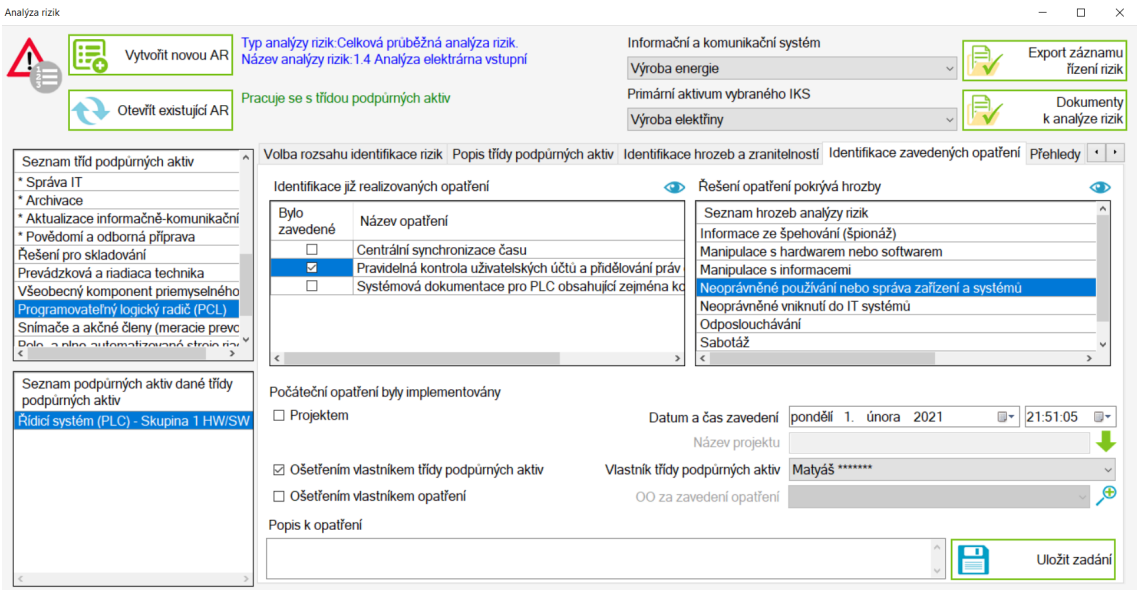
Metodika: Hrozby a zranitelnosti k jednotlivým aktivům definují jejich garanti v součinnosti s MKB. V **příloze 6 a 7** je seznam zranitelností a hrozeb relevantních pro elektrárnu vstupující do AR. Součástí analýzy rizik je identifikace konkrétních zavedených a nezavedených opatření ve společnosti.

ESKO implementace: Hrozby a zranitelnosti se identifikují v kartě „Analýza rizik". Výběrem třídy podpůrných aktiv, respektive podpůrného aktiva se zobrazí hrozby působící potenciálně na zvolené podpůrné aktivum. Po kliknutí na jednotlivou hrozbu se zobrazí slabiny aktiva, kterých mohou hrozby využít, tedy jejich zranitelnosti. Kliknutím na zranitelnost se zobrazí možná opatření k eliminaci hrozeb. Na obrázku 26 je vidět příklad namapovaných hrozeb, zranitelností a opatření ke konkrétnímu zvolenému podpůrnému aktivu.



Obrázek 26: Identifikace hrozeb a zranitelností AR (Zdroj: Nástroj ESKO)

V záložce „Identifikace zavedených opatření“ ve spolupráci s garanty určuji opatření, která byla aplikována v čase tvoření analýzy rizik (obrázek 27).



Obrázek 27: Identifikace zavedených opatření AR (Zdroj: Nástroj ESKO)

V záložce „Přehledy“ je souhrn dosud identifikovaných hrozeb, zranitelností a (ne)aplikovaných opatření vázaných na dílčí aktiva.

Postup je pro lepší pochopení zobrazen vývojovým diagramem v **příloze 8**.

Hodnocení rizik

Metodika: Rizika hodnotí garanti jednotlivých aktiv. V ESKO je použita doporučená metodika pro hodnocení rizik VKB.

Hodnota výsledného rizika (R) se určí jako součin hodnoty aktiva (A), pravděpodobnost realizace hrozby (T) a míry zranitelnosti (V). Při hodnocení je zohledňované i existující bezpečnostní opatření související s daným rizikem (5).

Hodnotu rizik lze tedy vypočítat dle vzorce (5):

$$\mathbf{R = A * T * V}$$

Hodnoty hrozby, zranitelnosti se stanovuje podle tabulek 9 a 10. K jednotlivým stupňům je přiřazen i slovní popis.

Tabulka 9: Stupnice hodnocení hrozeb (Zdroj: (5))

Úroveň	Popis
Nízká	Hrozba je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Tabulka 10: Stupnice hodnocení zranitelností (Zdroj: (5))

Úroveň	Popis
Nízká	Zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Úroveň rizika se hodnotí podle matice zobrazené v tabulce 11.

Tabulka 11: Matice hodnocení úrovně rizika (Zdroj: Vlastní zpracování dle (5))

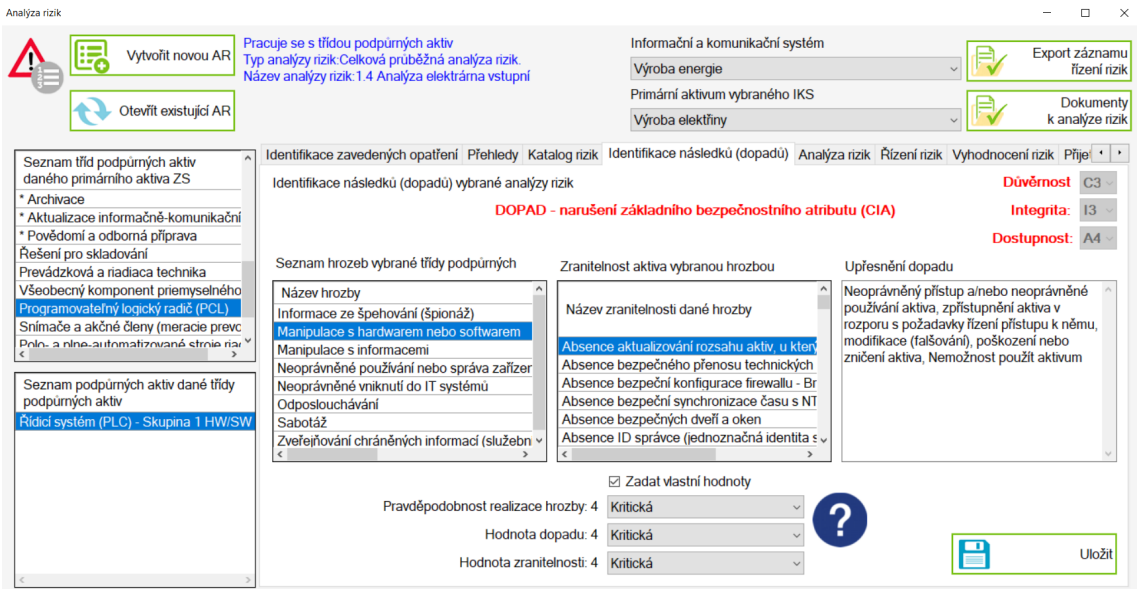
			Úroveň hrozby (T)															
			Nízká (velice nepravděpodobná realizace hrozby) [1]				Střední (málo pravděpodobná až pravděpodobná) [2]				Vysoká (pravděpodobná až velmi pravděpodobná) [3]				Kritická (velmi pravděpodobná až jistá) [4]			
			Úroveň zranitelnosti (V)				Úroveň zranitelnosti (V)				Úroveň zranitelnosti (V)				Úroveň zranitelnosti (V)			
			Nízká [1]	Střední [2]	Vysoká [3]	Kritická [4]	Nízká [1]	Střední [2]	Vysoká [3]	Kritická [4]	Nízká [1]	Střední [2]	Vysoká [3]	Kritická [4]	Nízká [1]	Střední [2]	Vysoká [3]	Kritická [4]
		TxV	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
Hodnota aktiva (A)	Nízké	1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	Střední	2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	Vysoké	3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	Kritické	4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Úroveň rizika je hodnocena dle stupnice v tabulce 12.

Tabulka 12: Stupnice pro hodnocení úrovně rizika (Zdroj: Vlastní zpracování dle (5))

Úroveň rizika	Označení pomocí písmen	přepočet		Popis + akceptovatelnost
		od	do	
Nízká	**D**	1	6	Riziko je považováno za akceptovatelné.
Střední	**C**	8	16	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoká	**B**	18	27	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritická	**A**	32	64	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

ESKO implementace: V ESKO se rizika hodnotí v kartě „Identifikace následků", kde se vybere aktivum, příslušná hrozba a na ni vázaná zranitelnost (obrázek 28). Výběrem se zobrazí atributy CIA, které byly narušeny využitím slabého místa hrozbou. Dále se zobrazí defaultně nastavené údaje míry pravděpodobnosti realizace hrozby, kvalifikace možného dopadu hrozby na zvolené primární aktivum a jeho zranitelnost. Tyto hodnoty lze měnit dle stupnice popsané v metodice výše (tabulka 9,10).

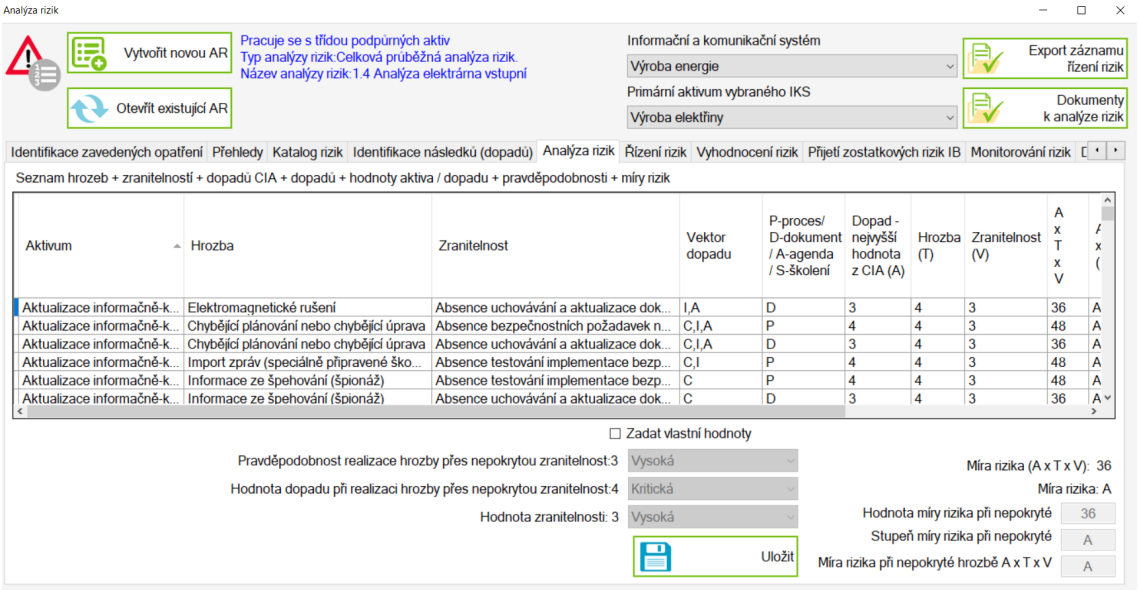


Obrázek 28: Hodnocení následků (dopadů) AR (Zdroj: Nástroj ESKO)

V záložce „Analýza rizik" jsou seskupeny informace z procházejících procesů:

- identifikace aktiv, kde jsou každému aktivu přiřazeny odpovídající hrozby a identifikovány zranitelnosti,
- stanovené možné dopady na tato aktiva z hlediska ohrožení důvěrnosti, dostupnosti a integrity primárních aktiv společnosti,
- určená míra pravděpodobnosti realizace scénáře, podle kterého hrozba využije neošetřenou zranitelnost příslušného aktiva.

V kartě lze provádět změny v hodnotě pravděpodobnosti realizace hrozby přes nepokrytou zranitelnost, dopadu při realizaci hrozby přes nepokrytou zranitelnost a hodnotě zranitelnosti. Záložka „Analýza rizik" je na obrázku 29.



Obrázek 29: Analýza rizik (Zdroj: Nástroj ESKO)

Řízení rizik

Metodika: Přijatelnost rizika je posuzována podle tabulky 12. Rizika, která jsou určena jako nepřijatelná, musí být ošetřena aplikací bezpečnostních opatření.

Výbor kybernetické bezpečnosti stanovuje kritéria pro akceptovatelnost rizik a výjimky akceptovatelnosti (5).

SW nástroj rozlišuje řízení rizik ve 4 úrovních

- **Řešení rizika** – spočívá v zavedení eliminačního opatření, která povedou k odstranění nebo snížení rizika na akceptovatelnou úroveň.
- **Přijetí rizika** – spočívá v akceptování identifikovaného rizika, používá se zejména v situaci, kdy ochranné, resp. eliminační opatření bylo nákladnější než případný dopad způsobený realizací rizika.
- **Vyhnutí se riziku** – pokud jsou identifikovaná rizika příliš vysoká, a/nebo jsou náklady na implementaci eliminačních opatření extrémně vysoké, přijme se opatření spočívající např. ve změně procesu nebo činností, podmínek, za nichž je činnost prováděna.
- **Sdílení rizika** – spočívá v rozhodnutí o sdílení rizik spolu s třetími stranami, příkladem může být např. pojištění nebo služby SLA, tj. poskytování podpory provozu třetí stranou se smluvním zajištěním (49).

ESKO implementace: V záložce „Řízení rizik“ se rozhoduje, jak má společnost s riziky identifikovanými v rámci analýzy rizik naložit. Po zvolení konkrétního rizika se posuzuje přijatelnost rizika dle možností uvedených v metodice.

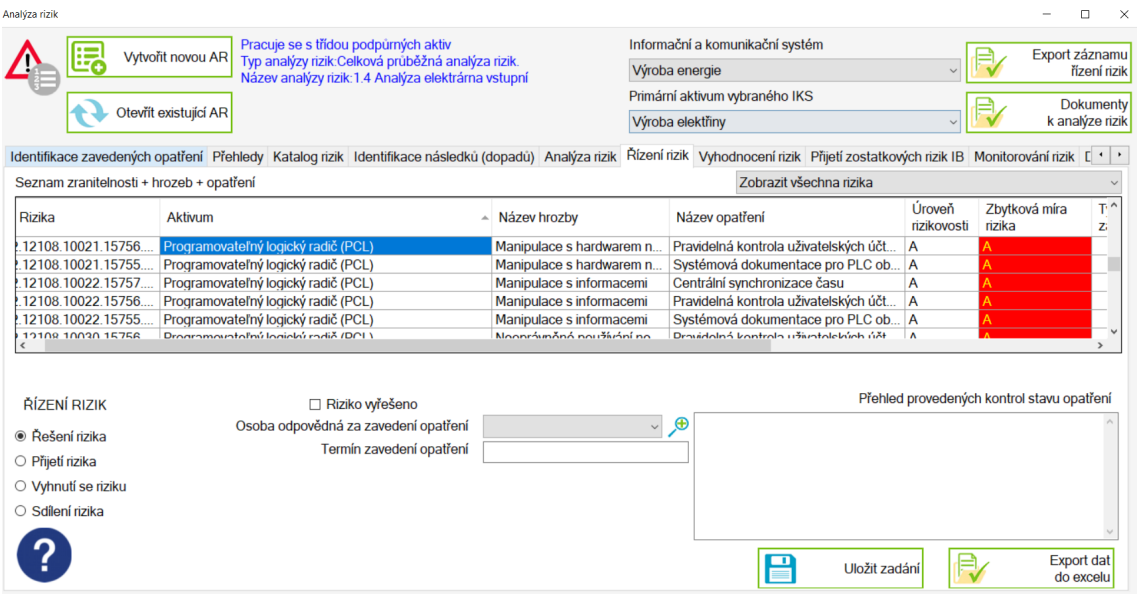
Při volbě **Řešení rizika** se doplní údaje o osobě odpovědné za zavedení opatření, termínu zavedení tohoto opatření a záznamy o provedených kontrolách. V případě, že je zvolena možnost „Riziko vyřešeno” objeví se ve sloupci „Úroveň rizikovosti” příznak „D”.

Při volbě **Přijetí rizika** je třeba doplnit údaje o osobě odpovědné za přijetí rizika, odůvodnění přijetí rizika, datum o rozhodnutí o přijetí rizika. Po vyplnění údajů se v souhrnné tabulce ve sloupci „Úroveň rizikovosti” objeví příznak „X” značící přijetí rizika.

Při volbě **Vyhnutí se riziku** je třeba doplnit údaje o osobě odpovědné za vyhnutí se riziku, způsobu zabránění riziku a datum rozhodnutí vyhnutí se riziku. Vyhnutí se riziku je v souhrnné tabulce zaznačeno příznakem „V”.

Při volbě **Sdílení rizika** se doplňují údaje o osobě odpovědné za sdílení rizika, osobě druhé strany odpovědné za sdílení rizika, popis způsobu sdílení rizika a datum rozhodnutí o sdílení rizik. V souhrnné tabulce je sdílení rizika značeno příznakem „Z”.

Na obrázku 30 je vidět záložka „Řízení rizik“.



Obrázek 30: Řízení rizik (Zdroj: Nástroj ESKO)

Zbylé záložky karty AR zobrazují přehledy identifikovaných rizik tříděných podle zavedených a nezavedených opatření a seznamy rizik tříděných podle způsobu akceptace rizika.

Výstup

Metodika: Prvotním výstupem procesu AR je zpráva o hodnocení rizik, která je MKB předložena Výboru kybernetické bezpečnosti, který rozhodne o akceptaci rizik. Po vyhotovení AR lze vygenerovat dokument prohlášení o aplikovatelnosti (PoA).

ESKO implementace: Zpráva o hodnocení rizik se vygeneruje po zvolení možnosti „Export záznamů řízení rizik". Příklady vygenerovaných sestav jsou v kapitole X.

Omezení rozsahu AR

Zadavatelem byla vyžadována pouze vstupní analýza. V následující fázi bude třeba vytvořit „průběžnou analýzu", která bude rozšířena o další realizovaná opatření a řízení rizik s detailnější specifikací podpůrných aktiv.

X. Příklady výstupních sestav

V této kapitole uvedu příklady výstupních sestav nástroje (Zpráva o stavu kybernetické bezpečnosti v organizaci a PoA – Prohlášení o aplikovatelnosti) naplňující různé pohledy na řízení kybernetické bezpečnosti. Vzhledem k rozsáhlosti výstupních materiálů dále uvádím pouze příklady výstupů k organizačním opatřením.

Manažerský pohled

Součástí zprávy je graf stavu oblasti organizačních opatření dle VKB (graf 1) zobrazující porovnání povinného rozsahu bezpečnostních opatření pro oblast organizačních opatření určených §3 až § 16 VKB a skutečného rozsahu aplikovaných bezpečnostních opatření ve společnosti. Hodnoty v grafu jsou uvedeny v procentech.

Graf 1: Stav oblasti organizačních opatření dle vyhlášky č. 82/2018 Sb. rizik (Zdroj: Nástroj ESKO)

Jak je z grafu 1 vidět, společnost splňuje se svými stávajícími organizačními opatřeními 50,5 % z množství požadovaného VKB.

Provozní pohled

Součástí výstupu je i seznam všech požadovaných (popřípadě zavedených) opatření spolu s hodnocením rizika. Přehled opatření následně slouží osobám odpovědným za zavádění opatření.

Na obrázku 31 jsou příklady požadovaných opatření v rámci řízení aktiv s nejvyšší možnou mírou rizika („A“).

Řízení aktiv

Vyhláška o kybernetické bezpečnosti č.82/2018 Sb., §4

Míra rizika
A

Kód opatření	Požadované opatření	MÍRA RIZIKA	MÍRA RIZIKA	Typ
VKB4P1j-a10	určení způsobů likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv	36	A	P
VKB4P2b-a12	Při hodnocení důležitosti primárních aktiv posouzení rozsahu dotčených právních povinností nebo jiných závazků,	36	A	P
VKB4P2c-a13	Při hodnocení důležitosti primárních aktiv posouzení rozsahu narušení vnitřních řídicích a kontrolních činností,	36	A	P
VKB4P2g-a17	Při hodnocení důležitosti primárních aktiv posouzení dopadů na zachování dobrého jména nebo ochranu dobré pověsti,	36	A	P
VKB4P2h-a18	Při hodnocení důležitosti primárních aktiv posouzení dopadů na bezpečnost a zdraví osob,	36	A	P
VKB4P2i-a19	Při hodnocení důležitosti primárních aktiv posouzení dopadů na mezinárodní vztahy a	36	A	P
VKB4P2j-a20	Při hodnocení důležitosti primárních aktiv posouzení dopadů na uživatele informačního a komunikačního systému.	36	A	P

Obrázek 31: Požadovaná opatření se stanovenou mírou (úrovní) rizika (Zdroj: Nástroj ESKO)

Na obrázku 32 je seznam identifikovaných rizik, která jsou rozdělena podle jednotlivých typů opatření.

STRUKTURA IDENTIFIKOVANÝCH NEPOKRYTÝCH RIZIK PODLE TYPU OPATŘENÍ

Typy opatření	Počet opatření ze skupiny
Rizika nepokrytá opatřeními typu **A** (Fyzická realizace)	**145**
Rizika nepokrytá opatřeními typu **P** (Proces)	**595**
Rizika nepokrytá opatřeními typu **D** (Dokument)	**95**
Rizika nepokrytá opatřeními typu **S** (Školení)	**4**

10 HROZEB S NEJVYŠŠÍM POČTEM NEOŠETŘENÝCH ZRANITELNOSTÍ	Počet eliminačních opatření
Neoprávněné vniknutí do IT systémů (G.0.23)	**132**
Porušení zákonů anebo předpisů (G.0.29)	**127**
Chybějící plánovaní anebo chybějící úprava (G.0.18)	**112**
Neoprávněné užití anebo správa zařízení a systémů G.0.30	**112**
Ztráta integrity citlivých informací (G.0.46)	**93**
Nesprávné žití anebo správa zařízení a systémů (G.0.31)	**90**

SEZNAM HROZEB	Počet eliminačních opatření
Neoprávněné vniknutí do IT systémů (G.0.23)	**132**
Porušení zákonů anebo předpisů (G.0.29)	**127**
Chybějící plánovaní anebo chybějící úprava (G.0.18)	**112**
Neoprávněné užití anebo správa zařízení a systémů G.0.30	**112**
Ztráta integrity citlivých informací (G.0.46)	**93**
Nesprávné žití anebo správa zařízení a systémů (G.0.31)	**90**

Obrázek 32: Seznam a počet nepokrytých rizik (Zdroj: Nástroj ESKO)

Opatření označené *Fyzická realizace (*„A“), je opatření určené k okamžité realizaci/implementaci (např. implementace firewallu). Opatření označené *Proces* („P“), je soubor opakujících se, časově rozložených činnosti a postupů určených pro identifikaci, popsání, evidování, zkoumání a eliminování příslušných rizik. Opatření označené *Dokument* („D“), je opatření písemné povahy (nařízení, směrnice, dokumentované procesy a postupy, záznamy apod.), které je v této podobě šířeno a aplikováno. Opatření označené *Školení* („S“) je opatření edukačního rázu, které je přímo navázané na zaměstnance organizace, pracovníky třetích stran.

Auditní pohled

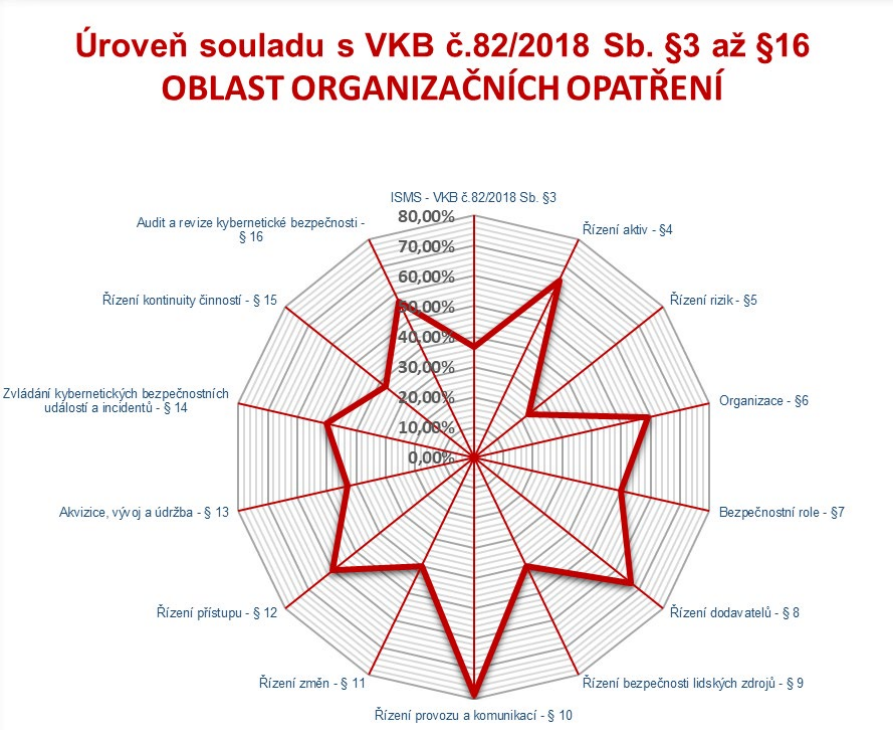
Součástí zprávy je také tabulka a graf úrovně souladu s VKB sloužící zejména pro externí i interní audity.

Úroveň souladu nebo také stav aplikování organizačních opatření v rámci jednotlivých procesů, respektive paragrafů VKB je zaznamenána v následující tabulce 13.

Tabulka 13: Úroveň souladu s VKB (Zdroj: Nástroj ESKO)

	Název oblasti opatření dle VKB	Skutečný stav zabezpečení
Oblast organizačních opatření	ISMS – VKB č.82/2018 Sb. §3	**36,36 %**
	Řízení aktiv – §4	**65,00 %**
	Řízení rizik – §5	**23,08 %**
	Organizace – §6	**59,09 %**
	Bezpečnostní role – §7	**50,00 %**
	Řízení dodavatelů – §8	**66,67 %**
	Řízení bezpečnosti lidských zdrojů – §9	**40,00 %**
	Řízení provozu a komunikací – §10	**78,57 %**
	Řízení změn – §11	**40,00 %**
	Řízení přístupu – §12	**60,00 %**
	Akvizice, vývoj a údržba – §13	**42,86 %**
	Zvládání kybernetických bezpečnostních událostí a incidentů - §14	**50,00 %**
	Řízení kontinuity činností – §15	**37,50 %**
	Audit a revize kybernetické bezpečnosti – §16	**57,14 %**

Tento soulad je ve zprávě znázorněna i pomocí pavučinového grafu (graf 2).



Graf 2: Grafického vyjádření úrovně souladu organizačních procesů s VKB č. 82/2018 Sb. §3 až §16 (Zdroj: Nástroj ESKO)

Z grafu je zřejmé, že nejvyšší soulad v oblasti organizačních opatření je ve společnosti zajištěn v rámci řízení provozu a komunikací (§10). Naopak nejvíce opatření bude potřeba zavést v rámci řízení rizik (§5).

Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti ve smyslu požadavků VKB se skládá ze dvou částí:

- přehledu vyloučených bezpečnostních opatření požadovaných touto vyhláškou včetně zdůvodnění, proč nebyla aplikována,
- přehledu zavedených bezpečnostních opatření včetně způsobu jejich implementace (5).

Na obrázku 33 je ukázána forma výstupu PoA v případě vyloučení opatření. Příkladem je zde vyloučené opatření spadající do řízení provozu a komunikací, které bylo vyloučeno z důvodu nerelevance v analyzovaném prostředí.

1. PŘEHLED VYLOUČENÝCH OPATŘENÍ[11]

Název aktiva:

Řízení provozu a komunikací

Vyhláška o kybernetické bezpečnosti č.82/2018 Sb., §10

Kód opatření	Vyloučené opatření			MIRA RIZIKA	MIRA RIZIKA	Typ
VKB10P3-a14	Oddělení vývojového, testovacího a provozního prostředí			9	C	A
Po jeho řízení				9	V	
Způsob řízení	Vyhnutí se riziku					
Důvod	Není relevantní pro dané prostředí.					
Odpovědná osoba	**********	Datum rozhodnutí	10. 2. 2021			

Obrázek 33: Přehled vyloučených opatření (Zdroj: Nástroj ESKO)

Na obrázku 34 je příklad přehledu zavedených opatření typu proces.

Seznam zavedených opatření typu PROCES

Kód opatření	Zavedená opatření typu: PROCES	MIRA RIZIKA	MIRA RIZIKA	Typ
VKB3Pd-a4	řízení rizik	9	C	P
VKB3Pe2-a6	stanovení bezpečnostní politiky v dalších oblastech podle § 30 a zavedení přiměřené bezpečnostní opatření	9	C	P
VKB4P1c-a3	Identifikace a evidování aktiv	9	C	P
VKB4P1d-a4	Určení a evidování garanty aktiv	9	C	P
VKB4P1e-a5	Hodnocení a evidování primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a zařazení jich do jednotlivých úrovní	6	D	P
VKB4P1f-a6	Určení a evidování vazeb mezi primárními a podpůrnými aktivy a hodnocení důsledků závislostí mezi primárními a podpůrnými aktivy	9	C	P
VKB4P1g-a7	Hodnocení podpůrných aktiv a zohledňování přitom zejména jejich vzájemné závislosti	9	C	P
VKB4P1h-a8	Stanovení a zavádění pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv na základě hodnocení aktiv	9	C	P
VKB4P1i-a9	Stanovení přípustných způsobů používání aktiv a pravidla pro manipulaci s aktivy s ohledem na úroveň aktiv,	9	C	P
VKB4P2a-a11	Posuzování rozsahu a důležitosti osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství	9	C	P

Obrázek 34: Přehled zavedených opatření (Zdroj: Nástroj ESKO)

4.1.6 Zaškolení klíčových uživatelů ve využití nástroje

Garanti aktiv byli školeni v průběhu o použitých metodikách. Po dokončení implementace proběhlo školení garantů a MKB jako klíčových uživatelů SW nástroje, při kterém byli obeznámeni s funkcionalitami nástroje a výstupní dokumentací.

4.1.7 Ganttův diagram

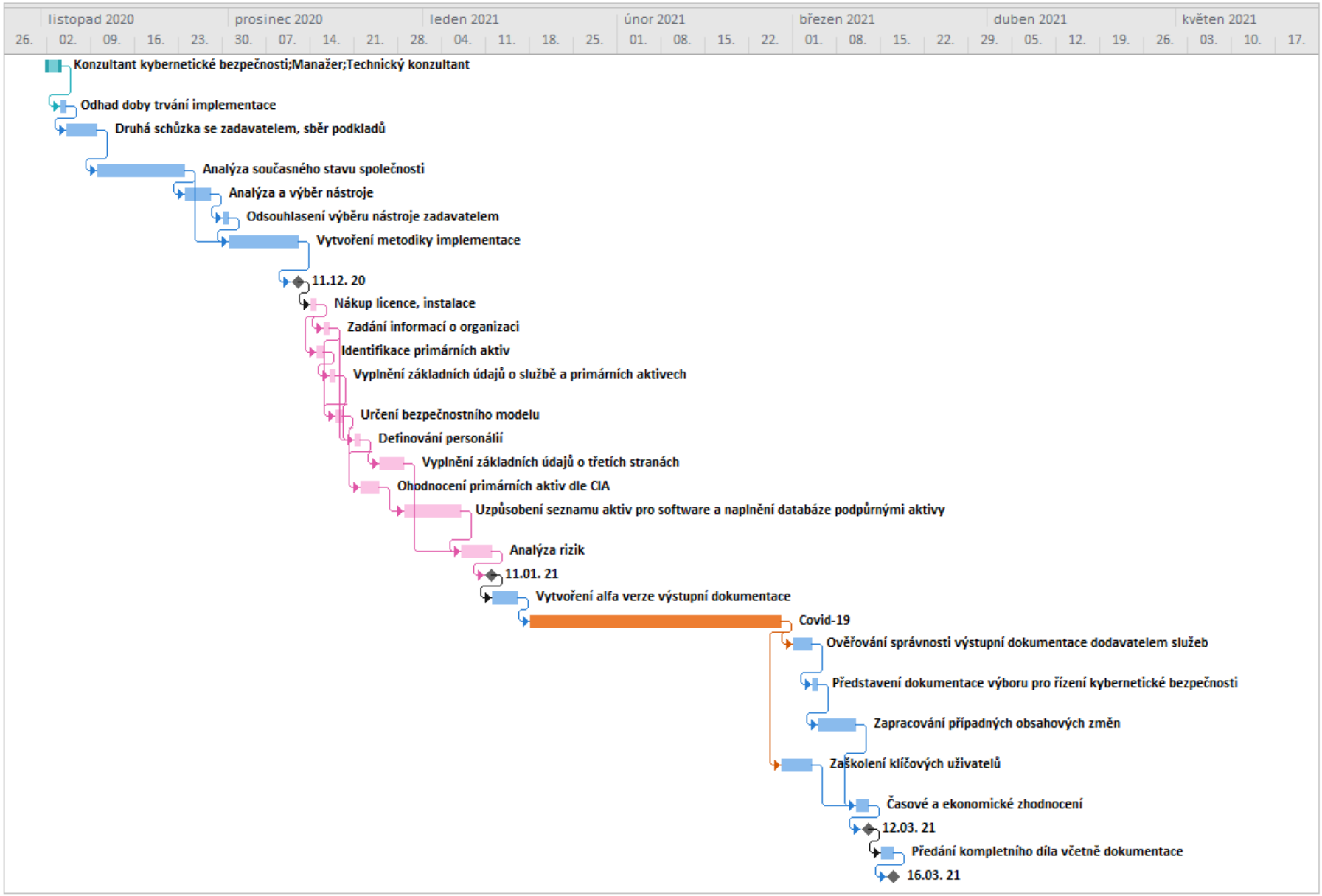
Pro stanovení skutečné doby trvání implementace byla provedena zpětná časová analýza s využitím Ganttova diagramu sestaveného pomocí programu Microsoft Project.

V tabulce 14 jsou uvedeny jednotlivé úkoly, jejich doba trvání, datum zahájení a dokončení jednotlivých úkolů a lidské zdroje vykonávající jednotlivé úkoly.

Tabulka 14: Činnosti v rámci realizace implementace s dobou trvání a lidskými zdroji (Zdroj: Vlastní zpracování v programu Microsoft Project)

	Název úkolu	Doba trvání	Zahájení	Dokončení	Předchůdci	Názvy zdrojů
1	Kick-off meeting	2 dny	02.11. 20	03.11. 20		Konzultant kybernetické bezpečnosti;Manažer; Technický konzultant
2	Odhad doby trvání implementace	1 den	04.11. 20	04.11. 20	1	Manažer
3	Druhá schůzka se zadavatelem, sběr podkladů	3 dny	05.11. 20	09.11. 20	2	Manažer;Konzultant kybernetické bezpečnosti; Technický konzultant
4	Analýza současného stavu společnosti	10 dny	10.11. 20	23.11. 20	3	Technický konzultant
5	Analýza a výběr nástroje	4 dny	24.11. 20	27.11. 20	4	Technický konzultant
6	Odsouhlasení výběru nástroje zadavatelem	1 den	30.11. 20	30.11. 20	5	Manažer
7	Vytvoření metodiky implementace	9 dny	01.12. 20	11.12. 20	6;4	Konzultant kybernetické bezpečnosti; Technický konzultant
8	***Ukončení přípravné fáze***	0 dny	11.12. 20	11.12. 20	7	
9	Nákup licence, instalace	1 den	14.12. 20	14.12. 20	8	Technický konzultant
10	Zadání informací o organizaci	1 den	16.12. 20	16.12. 20	9	Technický konzultant
11	Identifikace primárních aktiv	1 den	15.12. 20	15.12. 20	9	Technický konzultant
12	Vyplnění základních údajů o službě a primárních aktivech	1 den	17.12. 20	17.12. 20	11	Technický konzultant
13	Určení bezpečnostního modelu	1 den	18.12. 20	18.12. 20	10;12	Technický konzultant
14	Definování personálií	1 den	21.12. 20	21.12. 20	10;12	Technický konzultant
15	Vyplnění základních údajů o třetích stranách	2 dny	25.12. 20	28.12. 20	14	Technický konzultant
16	Ohodnocení primárních aktiv dle CIA	3 dny	22.12. 20	24.12. 20	13;14	Technický konzultant
17	Uzpůsobení seznamu aktiv pro software a naplnění databáze podpůrnými aktivy	7 dny	29.12. 20	06.01. 21	16	Technický konzultant
18	Analýza rizik	3 dny	07.01. 21	11.01. 21	17;15	Technický konzultant
19	***Ukončení implementace***	0 dny	11.01. 21	11.01. 21	18	
20	Vytvoření alfa verze výstupní dokumentace	4 dny	12.01. 21	15.01. 21	19	Technický konzultant
21	**Covid-19**	30 dny	18.01. 21	26.02. 21	20	
22	Ověřování správnosti výstupní dokumentace dodavatelem služeb	3 dny	01.03. 21	03.03. 21	21	Konzultant kybernetické bezpečnosti
23	Představení dokumentace výboru pro řízení kybernetické bezpečnosti	1 den	04.03. 21	04.03. 21	22	Manažer
24	Zapracování případných obsahových změn	4 dny	05.03. 21	10.03. 21	23	Technický konzultant; Konzultant kybernetické bezpečnosti
25	Zaškolení klíčových uživatelů	3 dny	26.02. 21	03.03. 21	21	Konzultant kybernetické bezpečnosti; Technický konzultant
26	Časové a ekonomické zhodnocení	2 dny	11.03. 21	12.03. 21	24;25	Manažer
27	***Odsouhlasení výstupů zadavatelem***	0 dny	12.03. 21	12.03. 21	26	
28	Předání kompletního díla včetně dokumentace	2 dny	15.03. 21	16.03. 21	27	Manažer
29	***Akceptace díla***	0 dny	16.03. 21	16.03. 21	28	

Grafické zobrazení tabulky 14 pomocí Ganttova diagramu je vidět na obrázku 35.



Obrázek 35: Ganttův diagram implementace ESKO (Zdroj: Vlastní zpracování)

Na Ganttově diagramu (obrázek 35) jsou růžově zaznačeny činnosti, které byly provedeny pomocí nástroje ESKO, modře jsou zobrazeny ostatní činnosti, které bylo nutné provést k úspěšné implementaci nástroje.

Implementace probíhala za specifických podmínek způsobených koronavirovou pandemií a nouzového stavu, což vedlo k prodlení některých fází implementace, zejména těch vyžadující osobní setkání.

Celková doba trvání byla 97 dní. Z toho 30 dní prodleva způsobená koronavirovou pandemií (v diagramu vyznačená oranžově). Do ekonomického hodnocení tedy vstupuje doba trvání po odečtení této prodlevy, tedy 67 dní.

5 EKONOMICKÉ ZHODNOCENÍ ZVÝŠENÍ BEZPEČNOSTI

V rámci ekonomického zhodnocení se zabývám návratností investice do zvýšení bezpečnosti prostřednictvím implementace nástroje ESKO. Finanční zdroje vynaložené na koupi licence a implementaci nástroje porovnávám s možnou finanční ztrátou v důsledku bezpečnostního incidentu nebo plynoucí ze sankcí vyplývajících z neplnění zákonných požadavků.

Pokud kontrolní orgán (NÚKIB) při auditu zjistí nedostatky, uloží společnosti, aby je napravila, a určí lhůtu na zavedení nápravných opatření, popřípadě i způsob nápravy. V případě zjištění bezprostředního ohrožení informačního systému kritické infrastruktury bezpečnostním incidentem může dokonce zakázat užívání informačního systému nebo jeho části do té doby, než bude zavedeno nápravné opatření. Provozovateli informačního a komunikačního systému kritické infrastruktury dále hrozí v případě nezavedení, respektive neprovádění bezpečnostních opatření nebo nevedení bezpečnostní dokumentace pokuta do výše 5 mil. Kč, která může být udělena i opakovaně (15).

Pro ekonomické zhodnocení realizované implementace jsem zvolila metodiku bezpečnostní agentury ENISA *Introduction to Return on Security Investment* (2), která rozebírá problematiku ekonomického hodnocení návratnosti investic do bezpečnostních opatření.

Exaktní měření efektivity vynaložených nákladů v oblasti bezpečnosti informací naráží na některé obtíže. Klíčovým úskalím jakékoli metodiky hodnocení návratnosti bezpečnostních investic je fakt, že se nejedná o běžný ekonomický výpočet poměru výnosů, nákladů a výsledného profitu. Jedná se o výpočet efektivity prevence potenciální ztráty (tj. kolik z potenciální ztráty by mohla investice ušetřit).

Výpočet navržený ENISA spočívá v porovnání peněžní hodnoty investice s peněžní hodnotou snížení rizika. Tuto peněžní hodnotu rizika lze odhadnout kvantitativním posouzením rizika.

Metodika pracuje s pojmem návratnosti investice do zabezpečení ROSI (*Return on Security Investment*). Metodika ROSI rozšiřuje obecně rozšířenou metodiku ROI (*Return on Investment*), kterou je v principu možno využít pro výpočet návratnosti jakékoli investice. Cílem rozšířené metodiky ROSI je snaha zhodnotit adekvátnost specifického typu investice do zabezpečení.

Vstupní předpoklady výpočtu ROSI

Nejdříve je nutno stanovit některé nezbytné vstupní předpoklady:

Jednotková očekávaná ztráta (Single Loss Expectancy, SLE) – jedná se o očekávaný finanční objem ztráty, pokud se zrealizuje bezpečnostní riziko. Jde o vyčíslení celkové ztráty při jednotlivém výskytu incidentu, do kterého by měly být zahrnuty všechny známé faktory s vlivem na výslednou cenu ztráty, aby se předešlo (v praxi obvyklému) podcenění ztráty (2).

Roční míra výskytů (Annual Rate of Occurrence, ARO) – jedná se o míru pravděpodobnosti, že se dané riziko zrealizuje v období jednoho roku. Stanovení této míry vyžaduje schopnost aproximace z více různých informačních zdrojů. V některých případech je nutno se spolehnout na tzv. zkušenostní odhad (2).

Roční očekávaná ztráta (*Annual Loss Expectancy, ALE*) – tato hodnota se vypočítává z obou předchozích hodnot dle vzorce (2):

$$ALE = SLE * ARO$$

Stanovení MR a výpočet MLR

Finančně vyjádřená redukce ztráty (Monetary Loss Reduction, MLR) – je finančně vyjádřené pravděpodobné snížení ztráty v důsledku uplatnění opatření. Jako praktická pomůcka pro výpočet MLR se využívá ukazatel tzv. *redukce rizika (Mitigation Ratio, MR)* – jedná se o procentuálně vyjádřenou částku, která vyjadřuje, o jaký relativní poměr dokáže dané opatření snížit nebezpečí dopadu rizika. MLR se vypočítá dle vzorce (2):

$$MLR = ALE * MR$$

Výpočet ukazatele ROSI

Návratnost investice do bezpečnostního opatření (Return on Security Investment, ROSI) – jedná se o výsledný vypočítávaný ukazatel metodiky. Vzorec pro výpočet ROSI vychází z analogického výpočtu ROI (2):

$$ROSI = (MLR - Náklady\ na\ opatření)/Náklady\ na\ opatření,$$

kde *náklady na opatření* jsou součtem všech finančních nákladů vynaložených na pořízení a implementaci bezpečnostních opatření.

Výsledná částka ROSI je vyjádřena v procentech a reprezentuje poměr návratnosti vynaložených nákladů na snížení rizika (2).

Limity ukazatele ROSI

Jak je jistě zřetelné z předchozího popisu výpočtu ROSI, některé vstupní ukazatele mohou být stanoveny chybně nebo nepřesně a mohou tak snížit relevanci získaného výsledku. Jedná se tedy zčásti o kvalifikovaný odhad nikoli o plně exaktní výpočetní metodu. Výsledek je možné dále zpřesňovat na základě využití dostupných statistických údajů, pokud v dané oblasti jsou k dispozici. Tam kde podobná data nemáte k dispozici, mohou v některých specifických případech existovat např. best practice standardy, které umožní přesněji stanovit například hodnoty ARO apod. Každé podobné zpřesnění je užitečné (2).

Limity zde realizovaného výpočtu ukazatele ROSI

Z hlediska započtených nákladů byla v této práci použita abstrakce jako kdyby se investice (náklad) na implementaci ESKO celá finančně realizovala v jednom roce, a to v roce pořízení. V letech následujících sice náklady na provoz ESKO nebudou nulové, ale budou nižší než cena pořízení v prvním roce a návratnost investice tak bude za delší časové období výrazně vyšší než v prvním roce (respektive ve zde provedeném výpočtu).

Do nákladů na pořízení bezpečnostního opatření nejsou započteny vlastní náklady na straně objednatele (časové a mzdové náklady apod.). Jejich případné započtení by naopak výslednou efektivitu investice o něco snížilo.

Tato omezení jsou dána jednak snahou o zachování jednoduchosti a transparentnosti výpočtu a dále pak chybějícími vstupními údaji.

Výsledný ukazatel ROSI je záměrně vypočítán pro každý z incidentů zvlášť, za účelem porovnání návratnosti investice do nástroje ESKO při různých typech incidentu.

V následujících tabulkách jsou uvedeny všechny potřebné hodnoty a výpočty pro stanovení ROSI.

Tabulka 15: Souhrn implementačních nákladů na bezpečnostní systém (Zdroj: Vlastní zpracování)

Označení	*Detailní popis*	*Cena (bez DPH) v Kč*
Licence ESKO	Nákup licence softwarového nástroje ESKO	26 850,00
Implementace ESKO	Implementace softwarového nástroje ESKO	261 500,00
Školení ESKO	Školení klíčových uživatelů ve využití ESKO	36 450,00
Náklady celkem		**324 800,00**

Tabulka 16: Typy incidentů (Zdroj: Vlastní zpracování)

Označení	*Detailní popis*	*Ztráta (SLE)v Kč*	*Výskyt (ARO)*	*Roční ztráta (ALE) v Kč*
Výpadek služby	Jednodenní výpadek služby (primárního aktiva) způsobený úspěšným útokem*	8 000 000,00	0,4	3 200 000,00
Pokuta NÚKIB	Pokuta NÚKIB (horní) v důsledku nezavedení opatření (pro KII)	5 000 000,00	0,7	3 500 000,00

** jedná se o záměrně abstrahované číslo z důvodu anonymizace s dodržením reálného číselného řádu*

Tabulka 17: Bezpečnostní opatření (Zdroj: Vlastní zpracování)

Označení	*Detailní popis*
Evidence IT aktiv	Zavedení transparentní evidence IT aktiv (implementace a konfigurace ESKO)
Definování rolí	Definování rolí a zodpovědností v oblasti bezpečnosti aktiv (konfigurace ESKO)
Analýza rizik	Analýza bezpečnostních rizik (konfigurace a výstupy ESKO)
Dokumentování	Zavedení procesu dokumentování podle zákona pomocí nástroje ESKO (pro KII)
Školení ESKO	Vyškolení personálu pro práci s aktivy, bezpečnostními rolemi a nástrojem ESKO

Tabulka 18: Hodnocení rizik (Zdroj: Vlastní zpracování)

Incident:	Výpadek služby	Pokuta NÚKIB
Opatření	*Redukce rizika (MR) v %*	*Redukce rizika (MR) v %*
Evidence IT aktiv	30	85
Definování rolí	10	80
Analýza rizik	35	85
Dokumentování	5	90
Školení ESKO	20	75
Průměr (MR)	**20**	**83**

Tabulka 19: Finanční vyjádření redukce rizika (Monetary Loss Reduction) (Zdroj: Vlastní zpracování)

Incident	*Redukce rizika (MLR) v Kč*
Výpadek služby	640 000,00
Pokuta NÚKIB	2 905 000,00
Celkem	**3 545 000,00**

Tabulka 20: Výpočet ukazatele ROSI (Return on Security Investment) (Zdroj: Vlastní zpracování)

Incident	*Redukce rizika (MLR) v Kč*	*Náklady na opatření v Kč*	*ROSI v %*
Výpadek služby	640 000,00	324 800,00	**97**
Pokuta NÚKIB	2 905 000,00	324 800,00	**794**

Klíčový účinek nasazení nástroje se předpokládá v oblasti legislativních povinností (viz tabulka výše „Pokuta NÚKIB"). V tomto případě, se výsledná návratnost bezpečnostní investice ROSI zdola blíží osminásobku investované částky a dá se tak

považovat za mimořádně efektivní. U druhého typu incidentu (viz tabulka výše „Výpadek služby”) je investice o řád méně efektivní. Tento incident však slouží zejména k porovnání.

Z výsledků vyplývá, že investice do zabezpečení je celkově návratná a společnosti se tato investice vyplatí. Zejména pak v případě incidentu, kvůli kterému je nástroj hlavně zaváděn, tedy pokutě od NÚKIB při případném auditu.

ZÁVĚR

Hlavním cílem diplomové práce bylo vybrat a následně implementovat vhodný softwarový nástroj umožňující efektivní řízení kybernetické bezpečnosti ve společnosti. Společnost, ve které byl nástroj implementován, je určena prvkem kritické infrastruktury státu v oblasti výroby elektřiny a poskytování podpůrných služeb. Vzhledem možnému zařazení do kritické informační infrastruktury chce být společnost připravena plnit všechny legislativní požadavky a současně být připravena na audit NÚKIB.

Pro dosažení stanoveného cíle byla provedena analýza současného stavu společnosti. Informace byly získány formou řízených rozhovorů s garanty aktiv, s manažerem kybernetické bezpečnosti a studiem interních materiálů.

Na základě požadavků zadavatele byla stanovena kritéria pro výběr vhodného softwarového nástroje. Ze srovnání třech různých vybraných nástrojů nejlépe vyhověl stanoveným požadavkům nástroj ESKO. Nástroj byl schválen zadavatelem, konkrétně výborem pro řízení kybernetické bezpečnosti a následně byl také úspěšně implementován v základním rozsahu (vstupní analýza rizik). Vhodný výběr nástroje byl potvrzen v průběhu realizace, kdy se podařilo díky využití nástroje naplnit všechny požadavky zadavatele. Hlavní cíl práce se tedy podařilo splnit.

Dílčím cílem implementace byla příprava společnosti na případný audit od NÚKIB (dále jen audit). Po úspěšném naplnění databáze ESKO primárními a podpůrnými aktivy včetně jejich ohodnocení, vyplnění údajů o garantech aktiv, společnosti a třetích stranách, byla provedena analýza bezpečnostních rizik. Vyhotovení analýzy rizik umožňuje v nástroji ESKO vygenerovat bezpečnostní dokumentaci (PoA, zpráva o hodnocení rizik), která je nezbytným podkladem pro audit. Výstupní dokumentace byla schválena výborem pro řízení kybernetické bezpečnosti. Zároveň se společnost díky vedení bezpečnostní dokumentace a prostřednictvím zavádění opatření stanovených v rámci provedené analýzy rizik vyhne nebezpečí pokuty, která může být udělena při auditu v případě nedodržení povinností na základě zákona o kybernetické bezpečnosti (zákon č. 181/2014 Sb.).

Mezi další přínosy plynoucí z implementace ESKO nástroje patří zpřehlednění, automatizace a snadné udržování aktuálnosti dokumentace v oblasti řízení aktiv a rizik spolu s využitím postupů nejlepší praxe (best practice). Specializace nástroje

na průmyslové systémy usnadnila výběr relevantních bezpečnostních opatření. Zároveň bylo vyhověno požadavkům zadavatele na zefektivnění řízení kybernetické bezpečnosti, optimalizaci lidských zdrojů, zajištění souladu s legislativou a zefektivnění interního a externího auditu. Nástroj rovněž nabízí efektivní správu dokumentů.

Společnost plánuje v budoucnu použít přídavný modul pro řízení informační bezpečnosti. Také tomuto požadavku bylo vyhověno možností jednoduchého rozšíření ESKO nástroje o modul GDPR, který pomůže zajistit soulad s legislativou v oblasti ochrany a zpracování osobních a citlivých údajů.

Dílčím cílem návrhové části bylo vytvořit metodiku, podle které bude nástroj úspěšně implementován. Tento cíl se také podařilo splnit. Metodika byla tvořena s využitím doporučení vyhlášky o kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.), norem ISO/IEC 27000 a s využitím manuálu k nástroji. Stanovenou metodiku v této práci lze s mírnými úpravami použít jako obecně využitelný návod k implementaci nástroje ESKO.

Pro splnění všech výše uvedených cílů bylo nutno položit teoretický základ nezbytný pro pochopení problematiky, a to zejména v oblasti kybernetické bezpečnosti a jejího řízení. V teoretické části byly objasněny důležité pojmy v oblasti kybernetické bezpečnosti vycházející z české legislativy i z mezinárodních norem a vysvětlena specifika průmyslového prostředí a kritické (informační) infrastruktury.

Po stanovení činností a výstupů potřebných k naplnění cíle byla provedena časová analýza. Před vlastním zahájením implementace byla k prvotnímu odhadu doby trvání využita metoda síťové analýzy s určením kritické cesty v kombinaci s tzv. zkušenostními odhady (časové, kapacitní a termínové odhady z předchozích analogických projektů). Na závěr byla provedena zpětná časová analýza již uskutečněné realizace s využitím Ganttova diagramu a s využitím skutečných hodnot trvání dílčích kroků procesu implementace. Smyslem zpětné analýzy je získat co nejpřesnější podklady pro další zpřesňování časových analýz v budoucnu a podklady pro ekonomické zhodnocení. Oproti odhadované době trvání byla skutečná doba trvání delší zejména v důsledku protipandemických státních opatření (v důsledku tzv. covid-19), která zapříčinila posun některých činností vyžadujících osobní setkání. Reálně vynaložené kapacity byly o něco nižší, než byl původní předpoklad. K časové analýze před implementací i po implementaci byl využit Microsoft Project.

Cílem poslední kapitoly bylo ekonomicky zhodnotit náklady na pořízení licence nástroje ESKO a jeho implementaci společně s posouzením návratnosti investice. Ekonomické hodnocení ukázalo, že se společnosti vyplatilo investovat do implementace nástroje, a to zejména vzhledem k potřebě zajištění souladu s legislativním rámcem. Součástí realizace bylo také školení uživatelů v práci s ESKO.

Odsouhlasení všech výstupů zadavatelem potvrzuje úspěšné naplnění cílů definovaných v rámci této práce.

SEZNAM POUŽITÝCH ZDROJŮ

(1) LÉVY, Pierre. *Becoming virtual - reality in the Digital Age*. New York: Plenum Trade, 1998. ISBN 0-306-45788-1.

(2) *Introduction to Return on Security Investment: Helping CERTs assessing the cost of (lack of) security*. December 2012. Heraklion: European Network and Information Security Agency (ENISA). Dostupné také z: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment

(3) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary* [online]. Třetí aktualizované vydání. NCKB. Praha: Policejní akademie ČR v Praze, Česká pobočka AFCEA, 2015, 242 s. [cit. 2019-04-14]. ISBN ISBN 978-80-7251-436-6. Dostupné z: https://cybersecurity.cz/data/slovnik_v310.pdf

(4) Computer Security Resource Center: Glossary. *NIST: National Institute of Standards and Technology* [online]. Gaithersburg: NIST [cit. 2021-03-05]. Dostupné z: https://csrc.nist.gov/glossary

(5) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

(6) DOUCEK, Petr, Luděk NOVÁK, Vlasta SVATÁ a Lea NEDOMOVÁ. *Řízení bezpečnosti informací*. 2. rozšířené vydání o BCM. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

(7) KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. 1. vydání. Praha: CZ.NIC, 2019. CZ.NIC. ISBN ISBN978-80-88168-34-8.

(8) *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. Fifth edition. Geneva: International Organization for Standardization, 2018.

(9) Bezpečnost. In: *KYBEZ: Platforma kybernetické bezpečnosti* [online]. GORDIC, 2021 [cit. 2021-03-08]. Dostupné z: https://www.kybez.cz/bezpecnost

(10) LÉVY, Pierre. *Kyberkultura: zpráva pro Radu Evropy v rámci projektu "Nové technologie: kulturní spolupráce a komunikace"*. Praha: Karolinum, 2000. ISBN 80-246-0109-5.

(11) Národní strategie kybernetické bezpečnosti České republiky na období 2021-2025. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB, 2020 [cit. 2021-05-06]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

(12) Pojmosloví. In: *KYBEZ: Platforma kybernetické bezpečnosti* [online]. GORDIC, 2021 [cit. 2021-03-06]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

(13) WhatIs.com: Definitions. *TechTarget* [online]. Newton: TechTarget, ©1999–2021 [cit. 2021-03-06]. Dostupné z: https://whatis.techtarget.com/definitions/A

(14) KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, 2016. CZ.NIC, 14. publikace. ISBN 978-80-88168-18-8.

(15) ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů*. 2014, částka 75, č. 181. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014

(16) Legislativa KB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB, 2021 [cit. 2021-03-06]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

(17) *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Revision 2. Gaithersburg: National Institute of Standards and Technology, 2012. Special Publication 800-61. Dostupné také z: http://dx.doi.org/10.6028/NIST.SP.800-61r2

(18) O NÚKIB. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB, 2021 [cit. 2021-05-06]. Dostupné z: https://nukib.cz/cs/o-nukib/

(19) Kybernetická bezpečnost: NCKB. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB, 2021 [cit. 2021-05-06]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/

(20) O týmu CSIRT.CZ. *CSIRT.CZ* [online]. Praha: CZ.NIC, 2019 [cit. 2021-04-06]. Dostupné z: https://csirt.cz/cs/o-nas

(21) KROPÁČOVÁ, Andrea. CERT/CSIRT týmy a jejich role. In: *Root.cz* [online]. Praha: Root.cz, ©1998–2021 [cit. 2021-05-07]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

(22) MOYLE, Ed. *CERT vs. CSIRT vs. SOC: What's the difference?: What's in a name? Parse the true differences between a CERT, a CSIRT, a CIRT and a SOC, before you decide what's best for your organization.* [online]. 2021 [cit. 2021-02-24]. Dostupné z: https://searchsecurity.techtarget.com/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

(23) ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Druhé vydání. Praha: Úřad pro technickou normalizaci, meterologii a státní zkušebnictví, 2013. Třídící znak 369790.

(24) ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Druhé vydání. Praha: Úřad pro technickou normalizaci, meterologii a státní zkušebnictví, 2014. Třídící znak 369798.

(25) Bezpečnostní role a jejich začlenění v organizaci. In: *Podpůrné materiály* [online]. Verze 3.0. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2020 [cit. 2021-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

(26) ČESKÁ REPUBLIKA. Zákon č. 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů*. Praha, 2000, ročník 2000, částka 73, č. 240. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=240&r=2000

(27) ČESKÁ REPUBLIKA. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění nařízení vlády č. 315/2014 Sb. In: *Sbírka zákonů*. 2014, ročník 2014, částka 127, číslo 315. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=432&r=2010

(28) Schéma KII: Kritická informační infrastruktura. In: *Podpůrné materiály* [online]. Verze 2.0. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2021-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

(29) JORDÁN, Vilém a Viktor ONDRÁK. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. *Infrastruktura komunikačních systémů II: kritické aplikace*. Brno: Akademické nakladatelství CERM, 2015. ISBN 978-80-214-5240-4.

(30) SEDLÁK, Petr. *MCN* [prezentace]. Brno: Vysoké učení technické v Brně, 2021.

(31) PETR, Sedlák. *Bezpečnost ICS řešení* [prezentace]. Brno: Vysoké učení technické v Brně, 2016.

(32) NIST SP 800-82. *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other*

Control System Configurations such as Programmable Logic Controllers (PLC). Revision 2. Gaithersburg: National Institute of Standards and Technology, 2015. Dostupné také z: http://dx.doi.org/10.6028/NIST.SP.800-82r2

(33) CIEPIELA, Piotr. How to improve operational technology security and safety in LS. In: *EY* [online]. Ernst & Young, 2021 [cit. 2021-05-07]. Dostupné z: https://www.ey.com/en_cz/consulting/how-to-improve-operational-technology-security-and-safety-in-ls

(34) PROFIBUS Technology and Application - System Description. *Profibus: Profinet* [online]. Karlsruhe: PROFIBUS, 2020 [cit. 2021-05-07]. Dostupné z: https://www.profibus.com/download/profibus-technology-and-application-system-description

(35) POWERLINK: Real-time industrial Ethernet is reality. *B&R Industrial Automation* [online]. Eggelsberg: B&R Industrial Automation, 2021 [cit. 2021-05-07]. Dostupné z: https://www.br-automation.com/en/products/networks-and-fieldbus-modules/powerlink/

(36) Modbus FAQ: About the Protocol. *Modbus* [online]. Hopkinton: Modbus Organization, ©2005–2021 [cit. 2021-05-07]. Dostupné z: https://modbus.org/faq.php

(37) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

(38) *Interní dokumentace elektrárny*. Česká republika, 2020.

(39) Obchodní rejstřík, rejstřík firem v ČR, vztahy a vazby z justice.cz. *Kurzy CZ* [online]. ©2000–2021 [cit. 2021-04-10]. Dostupné z: https://rejstrik-firem.kurzy.cz

(40) *Výroční zpráva z roku 2020*. Česká republika, 2020.

(41) Technické normy: Seznam norem ČSN. *Technické normy ČSN* [online]. Hradec Králové: TECHNOR, ©2005–2018 [cit. 2021-05-11]. Dostupné z: http://www.technicke-normy-csn.cz/technicke-normy/

(42) ČESKÁ REPUBLIKA. Zákon č. 458/2000 Sb., o podmínkách podnikání a výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon). In: *Sbírka zákonů*. Praha, 2011, ročník 2000, částka 131, č. 211. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=211&r=2011

(43) Právní předpisy. *Úřad pro ochranu osobních údajů: the office do personal data protection* [online]. Praha: Úřad pro ochranu osobních údajů, 2013 [cit. 2021-04-19]. Dostupné z: https://www.uoou.cz/pravni-predpisy/ds-1257/archiv=0&p1=1657

(44) SEDLÁK, Petr. *ISMS: Zavádění a provozování ISMS Bezpečnostní projekt* [prezentace]. Brno: Vysoké učení technické v Brně, 2014.

(45) Software ESKO GDPR. *Sevitech CZ* [online]. Praha: SEVITECH CZ, 2020 [cit. 2021-05-08]. Dostupné z: https://www.sevitech.cz/software-gdpr-go/

(46) Predstavenie ISIT SOFTWARE SK. *ISIT SK software cybersecurity* [online]. Bratislava: ISIT Slovakia, 2020 [cit. 2021-05-08]. Dostupné z: https://www.gdpr-software.eu/predstavenie-isit-software-sk

(47) CSA: Řízení kybernetické bezpečnosti. *GORDIC: Kybernetická bezpečnost* [online]. Jihlava: GORDIC, 2021 [cit. 2021-05-08]. Dostupné z: https://gordiccybersec.cz/csa

(48) Řešení. *ZOTY* [online]. Zoty, 2020 [cit. 2021-05-08]. Dostupné z: https://zoty.cz/nase-reseni/

(49) *Manuál KBO ESKO CZ*. Bratislava: ISIT Slovakia, 2021. Interní dokument.

(50) Modul kybernetická bezpečnosť organizácie. In: *ISIT SK software cybersecurity* [online]. Bratislava: ISIT Slovakia, 2020 [cit. 2021-05-08]. Dostupné z: https://www.gdpr-software.eu/modul-kyberneticka-bezpecnost-organizacie?destination=node/489

(51) Systémové požiadavky. *ISIT SK software cybersecurity* [online]. Bratislava: ISIT Slovakia, 2020 [cit. 2021-05-08]. Dostupné z: https://www.gdpr-software.eu/systemove-poziadavky

(52) GRANNEMAN, Joseph. How to use the RACI matrix for a security risk assessment. In: *SearchSecurity: TechTarget* [online]. Newton: TechTarget, ©2000–2021 [cit. 2021-05-08]. Dostupné z: https://searchsecurity.techtarget.com/answer/How-to-use-the-RACI-matrix-for-a-security-risk-assessment

SEZNAM POUŽITÝCH ZKRATEK

ALE	Annual Loss Expectancy
API	Application Programming Interface
AR	Analýza rizik
ARO	Annual Rate of Occurrence
BIS	Bezpečnostní informační služba
BO	Bezpečnostní opatření
BOZP	Bezpečnost a ochrana zdraví při práci
CERT	Cyber Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CSA	Softwarový nástroj CyberSec
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
DCS	Distributed Control System
DPIA	Data Protection Impact Assessment
ENISA	The European Union Agency for Cybersecurity
EU	Evropské Unie
GDPR	General Data Protection Regulation
GovCERT.CZ	Vládní CERT
HW	Hardware
IB	Informační bezpečnost
ICS	Industrial Control System
ICT	Information and Communication Technology
IČO	Identifikační číslo osoby
ID	Identifier
IKS	Informační a komunikační systém
IP	Internet Protocol
IS	Informační systém
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO	International Organization for Standardization
IT	Information Technology
KBO	Kybernetická bezpečnost organizace
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
KZ	Krizový zákon
LAN	Local Area Network
MCN	Mission Critical Network
MKB	Manažer kybernetické bezpečnosti
MLR	Monetary Loss Reduction
MR	Mitigation Ratio
MSSQL	Microsoft SQL Server
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Restore/Recovery
NATO	The North Atlantic Treaty Organization (Severoatlantická aliance)
NCKB	Národní centrum kybernetické bezpečnosti České republiky
NCKO	Národní centrum kybernetických operací
NCOZ SKPV	Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování
NCPI	Network Critical Physical Infrastructure
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
OT	Operational Technology

PC	Personal Computer
PoA	Prohlášení o aplikovatelnosti
RAM	Random-access Memory
RASCI	Responsible, Accountable, Supportive, Consulted, Informed
ROI	Return on Investment
ROSI	Return on Security Investment
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SLA	Service-level Agreement
SLE	Single Loss Expectancy
SOC	Security Operations Center
SP	Special Publications
SQL	Structured Query Language
SR	Slovenská republika
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, Threats
TCP	Transmission Control Protocol
TMZV	Tuzemské ministerstvo zahraničních věcí
ÚZSI	Úřad pro zahraniční styky a informace
VeKySIO	Velitelství kybernetických sil a informačních operací
VKB	Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
VPN	Virtual Private Network
VZ	Vojenské zpravodajství
WAN	Wide Area Network
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ

SEZNAM PŘÍLOH